VISIONIAS
INSPIRING INNOVATION

SECURITY

Classroom Study Material 2026

June 2025 to April 2026

MAINS 365

AHMEDABAD | BENGALURU | BHOPAL | CHANDIGARH | DELHI | GUWAHATI | HYDERABAD | JAIPUR | JODHPUR | LUCKNOW | PRAYAGRAJ | PUNE | RANCHI

8468022022
9019066066

enquiry@visionias.in /c/VisionIASdelhi /visionias_upsc vision_ias /VisionIAS_UPSC www.visionias.in

"You are as strong as your Foundation"

FOUNDATION COURSE
GENERAL STUDIES
PRELIMS CUM MAINS

Approach is to build fundamental concepts and analytical ability in students to enable them to answer questions of Preliminary as well as Mains Exam

- Includes Pre Foundation Classes in 2027, 2028 & 2029
- Includes comprehensive coverage of all the topics for all the four papers of GS Mains, GS Prelims & Essay
- Access to LIVE as well as Recorded Classes on your personal student platform Includes All India GS Mains, GS Prelims, CSAT & Essay Test Series
- Our Comprehensive Current Affairs classes of PT 365 and Mains 365

Live - online / Offline Classes

Scan the QR CODE to download VISION IAS app

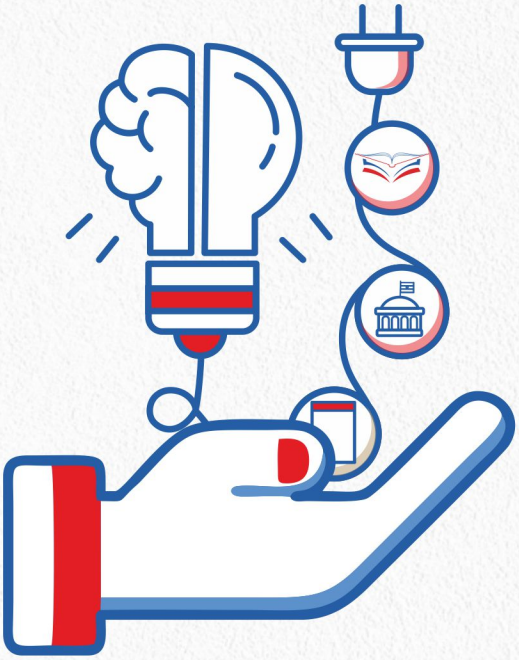
2027, 2028 & 2029

DELHI: 30 JUNE, 8 AM | 9 JULY, 11 AM | 16 JULY, 8 AM
22 JULY, 5 PM | 23 JULY, 11 AM | 24 JULY, 2 PM | 30 JULY, 8 PM

GTB NAGAR : 17 JULY, 6 PM | 19 JULY, 8 AM

AHMEDABAD: 15 JUNE | BENGALURU: 20 JULY | BHOPAL: 2 JUNE | HYDERABAD: 13 JULY
JAIPUR: 17 JUNE, 22 JUNE | JODHPUR: 15 MAY | LUCKNOW: 15 JULY | PUNE: 15 JULY

OPTIONAL SUBJECT CLASSES 2027



- Anthropology
- Geography
- Physics
- Sociology
- Public Administration
- Political Science and International Relations
- History
- Philosophy

Starts : 1 JULY

SECURITY

Table of Contents

1. STATE AND NON-STATE ACTORS _____ 5
1.1. Left-Wing Extremism (LWE) _____5
1.2. Armed Forces (Special Powers) Act (AFSPA) _____6
1.3. Insurgency in North East India _____8
1.4. High-Powered Demography Mission ____9
1.5. Keywords_____10
1.6. Practice Question _____10
2. THREATS TO INTERNAL SECURITY ____ 11
2.1. Technology and Internal Security _____11
2.1.1. Online Radicalisation _____11
2.1.2. Cryptocurrencies and Smuggling _____12
2.1.3. Emergence of AI in India's Internal Security Architecture _____13
2.1.4. Data Protection at a Glance _____16
2.1.5. Critical Information Infrastructure (CII) __17
2.2. Cybersecurity _____18
2.2.1. Cybercrime in India: Evolution, Threats and Strategic Responses _____18
2.2.2. Digital Sovereignty _____21
2.2.3. United Nations Convention Against Cybercrime _____22
2.2.4. Quantum Cyber Readiness _____22
2.3. Terrorism_____24
2.3.1. State-Sponsored Terrorism _____25
2.3.2. White Collar Terrorism_____25
2.4. Transnational Organized Crimes (TNOCs)28
2.5. Money Laundering and Smuggling ____29
2.5.1. Drug Trafficking _____30
2.6. Geospatial Data and National Security _31
2.7. Emerging Dimensions of Warfare _____32
2.7.1. Hybrid Warfare _____32
2.7.2. Grey-Zone Warfare Tactics _____ 33
2.7.3. Biosecurity and Biological Weapons Convention _____ 33
2.7.4. Space Weaponisation _____ 36
2.8. Keywords _____ 37
2.9. Practice Question _____ 37
3. SECURITY CHALLENGES AND THEIR MANAGEMENT IN BORDER AREAS _____ 38
3.1. Security Issues in Border Areas _____ 38
3.1.1. India and Bordering Countries _____ 38
3.2. Sudarshan Chakra Mission _____ 39
3.3. Quantum Technologies in Armed Forces40
3.4. Advance Technology & Border Management _____ 41
3.5. Keywords _____ 42
Practise Question _____ 42
4. MARITIME SECURITY AT A GLANCE____ 43
4.1. Defence Modernisation _____ 44
4.2. Theaterisation of Defence _____ 45
4.3. India's Joint Doctrine for Multi-Domain Operations _____ 46
4.4. Joint Doctrine for Cyberspace Operations47
4.5. Keywords _____ 49
4.6. Practise Question _____ 49
5. MISCELLANEOUS _____ 50
5.1. The Wassenaar Arrangement_____ 50
5.2. India's Defence Industry _____ 51
5.3. Keywords _____ 53
5.4. Practice Question _____ 53
6. APPENDIX: QUICK FACTS _____ 54

Copyright © by Vision IAS
All rights are reserved. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior permission of Vision IAS.

Preface

To the Aspirant Who Dares to Dream

Every year, thousands of aspirants prepare diligently for the UPSC Civil Services Examination with the dream of serving the nation. Among the papers that determine success in the Mains examination, General Studies Paper III often poses a unique challenge. While the syllabus appears limited, the nature of questions has evolved significantly. UPSC increasingly expects aspirants to go beyond conventional security issues and demonstrate an understanding of emerging threats, technological disruptions, institutional responses, and strategic policy measures.

Topics such as cyber security, Artificial Intelligence, quantum technologies, border management, hybrid warfare, terrorism, maritime security, and defence reforms are no longer isolated current affairs. They have become integral to India's national security architecture and demand a holistic understanding that combines static concepts with contemporary developments.

Recognising these evolving requirements, VisionIAS presents MAINS 365 – Security, a comprehensive and exam-oriented resource that consolidates one year's most relevant developments in Internal Security. The objective of this document is not merely to provide information but to help you understand issues from the perspective expected by UPSC, enabling you to write analytical, balanced and multidimensional answers.

We understand that aspirants often have several questions before relying on any resource. Let us address some of the most common ones.

Q1. There are numerous current affairs resources available. Why should I study Security from this document?

The challenge in Internal Security is not the lack of information but the abundance of scattered information spread across newspapers, PIB releases, committee reports, government documents and multiple magazines.

This document brings together the entire year's important developments into a single, integrated resource. Every topic has been carefully selected according to the UPSC syllabus and analysed from an examination perspective so that you spend less time collecting information and more time understanding and revising it.

Q2. UPSC increasingly asks analytical questions rather than factual ones. How does this document help?

UPSC no longer rewards aspirants who merely reproduce facts. It expects answers that explain issues comprehensively, analyse causes and consequences, evaluate government initiatives and present practical solutions.

Accordingly, every topic in this document has been structured to include:

- Why the issue is in news;
- Background and conceptual clarity;
- Dimensions and challenges;
- Government initiatives;
- Way Forward; and
- A balanced conclusion.

This systematic approach enables you to develop analytical answers instead of descriptive ones.

Q3. How does this document integrate Current Affairs with Static concepts?

One of the biggest challenges in General Studies Paper III is connecting current developments with the static syllabus.

This document consciously bridges that gap. Contemporary developments such as AI-driven policing, Quantum Cyber Readiness, Digital Sovereignty, Grey-Zone Warfare, Space Weaponisation and Cryptocurrencies have been explained alongside the relevant constitutional provisions, security doctrines, institutional mechanisms, international conventions and committee recommendations.

This integrated approach enables aspirants to enrich their answers with both conceptual understanding and current relevance.

Q4. Will this document help me write value-added answers in the examination?

Yes.

Each topic has been enriched with value addition through:

- authentic data and statistics;
- committee recommendations;
- government initiatives;
- international conventions;
- institutional mechanisms;
- best practices;
- relevant examples;
- keywords; and
- concise conclusions.

These elements significantly improve the quality, credibility and analytical depth of your answers.

Q5. How has information been presented to facilitate faster learning and revision?

The document has been designed keeping in mind the limited preparation time available before the Mains examination.

Instead of lengthy textual explanations, information has been organised through structured tables, diagrams, thematic flowcharts, comparison boxes, issue-based frameworks and visual summaries. Every page has been designed to maximise conceptual clarity while reducing cognitive load.

For instance, topics such as Left-Wing Extremism, Role of AI in India's Internal Security Architecture, AFSPA, Data Protection, Cybersecurity, Hybrid Warfare, and Border Management have been presented using visual frameworks that help aspirants quickly revise complex issues while retaining multidimensional understanding.

Q6. Security is a rapidly evolving subject. How comprehensive is the coverage?

The coverage extends well beyond traditional internal security topics.

Along with conventional issues such as terrorism, insurgency, border management and organised crime, this document includes emerging domains like:

• Artificial Intelligence in security;	• Quantum technologies;
• Cyber threats;	• Digital Sovereignty;
• Critical Information Infrastructure;	• Biosecurity;
• Space security;	• Grey-zone warfare;
• Maritime security;	• Defence modernisation;
• Multi-domain operations; and	• India's evolving defence ecosystem.

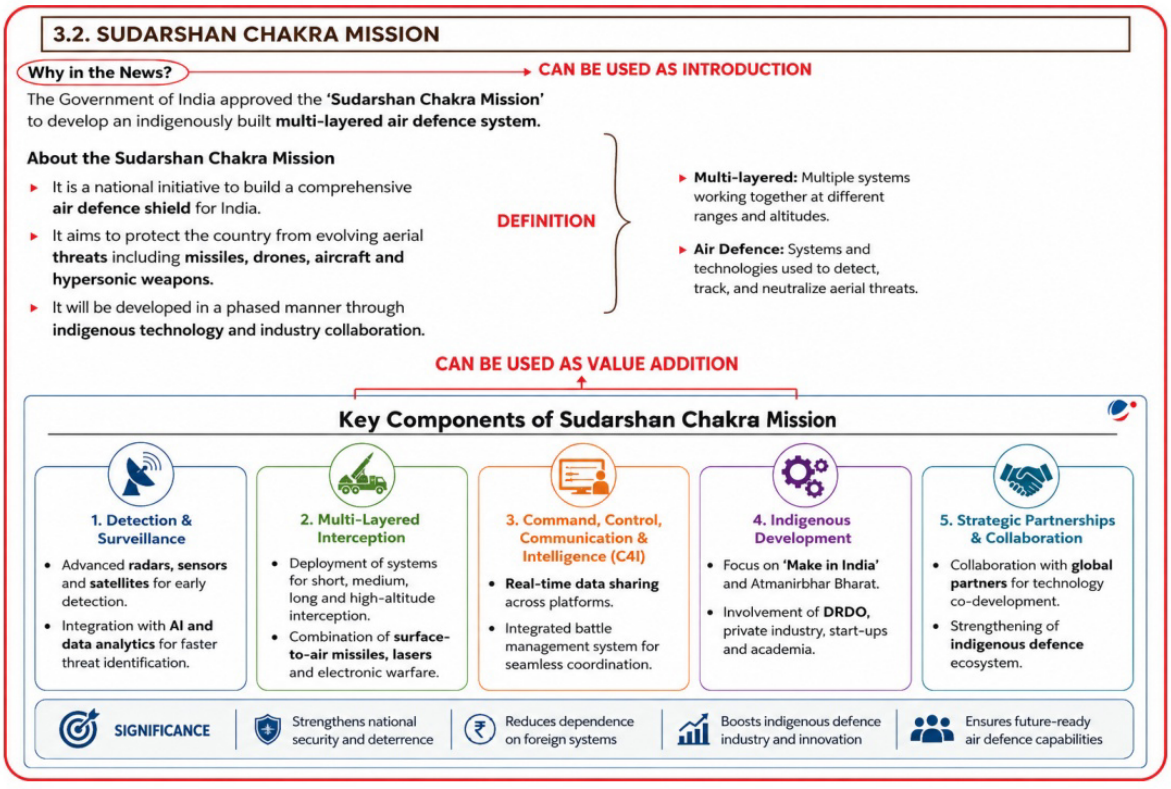
This ensures that aspirants remain prepared for both conventional and unconventional questions.

Q7. Will this document help in Answer Writing practice?

Certainly.

Beyond content enrichment, the document has been designed to familiarise aspirants with the structure expected in UPSC Mains.

Important keywords, issue-wise frameworks, balanced conclusions and answer-oriented presentation help aspirants organise their thoughts logically and present multidimensional answers within the time constraints of the examination.


3.2. SUDARSHAN CHAKRA MISSION
Why in the News?
CAN BE USED AS INTRODUCTION
The Government of India approved the 'Sudarshan Chakra Mission' to develop an indigenously built multi-layered air defence system.
About the Sudarshan Chakra Mission
It is a national initiative to build a comprehensive air defence shield for India.
It aims to protect the country from evolving aerial threats including missiles, drones, aircraft and hypersonic weapons.
It will be developed in a phased manner through indigenous technology and industry collaboration.
DEFINITION
Multi-layered: Multiple systems working together at different ranges and altitudes.
Air Defence: Systems and technologies used to detect, track, and neutralize aerial threats.
CAN BE USED AS VALUE ADDITION
Key Components of Sudarshan Chakra Mission
1. Detection & Surveillance
Advanced radars, sensors and satellites for early detection.
Integration with AI and data analytics for faster threat identification.
2. Multi-Layered Interception
Deployment of systems for short, medium, long and high-altitude interception.
Combination of surface-to-air missiles, lasers and electronic warfare.
3. Command, Control, Communication & Intelligence (C4I)
Real-time data sharing across platforms.
Integrated battle management system for seamless coordination.
4. Indigenous Development
Focus on 'Make in India' and Atmanirbhar Bharat.
Involvement of DRDO, private industry, start-ups and academia.
5. Strategic Partnerships & Collaboration
Collaboration with global partners for technology co-development.
Strengthening of indigenous defence ecosystem.
SIGNIFICANCE
Strengthens national security and deterrence
Reduces dependence on foreign systems
Boosts indigenous defence industry and innovation
Ensures future-ready air defence capabilities

Q8. How authentic and reliable is the content?

Every topic has been prepared after extensive research using authentic government publications, parliamentary committee reports, official policy documents, reputed international organisations and other credible institutional sources.

The focus has always been on accuracy, relevance and examination utility, ensuring that aspirants can confidently rely upon the content during their preparation.

Q9. How should I use this document for maximum benefit?

This document should not be viewed merely as a compilation of current affairs.

We recommend that aspirants:

- first develop conceptual clarity through the structured notes;
- connect each issue with the relevant GS Paper III syllabus;
- revise diagrams, keywords and frameworks regularly;
- supplement answer writing practice using the value-added content; and
- integrate the material with their static preparation.

Repeated revision using this approach will substantially improve both retention and answer quality.

Q10. What is our message to every aspirant?

The journey towards the Civil Services is demanding, but it is equally rewarding. Success belongs not merely to those who work hard, but to those who work consistently, revise intelligently and remain adaptable to the changing demands of the examination.

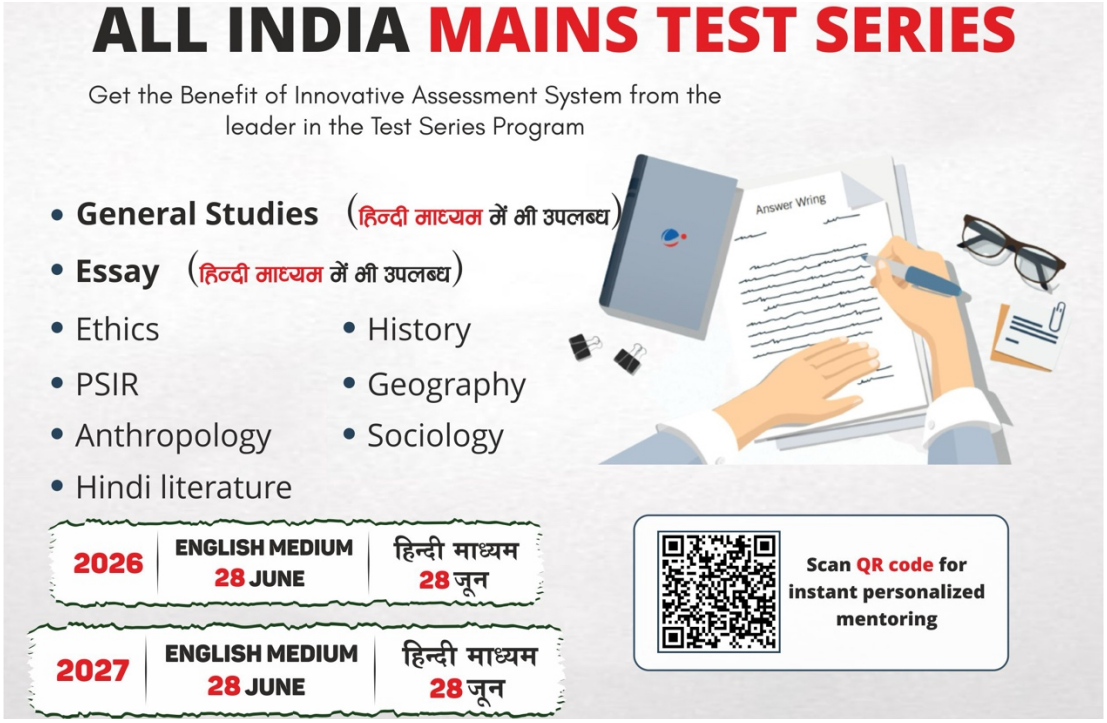
We hope that MAINS 365 – Security becomes a dependable companion in your preparation, helping you develop conceptual clarity, analytical ability and confidence to tackle one of the most dynamic sections of General Studies Paper III.

As always, we remain committed to supporting your journey with authentic, exam-oriented and high-quality learning resources.

We wish you the very best in your preparation and sincerely hope that your hard work culminates in success.

Happy Learning!

Team VisionIAS


ALL INDIA MAINS TEST SERIES
Get the Benefit of Innovative Assessment System from the leader in the Test Series Program
• General Studies (हिन्दी माध्यम में भी उपलब्ध)
• Essay (हिन्दी माध्यम में भी उपलब्ध)
• Ethics
• History
• PSIR
• Geography
• Anthropology
• Sociology
• Hindi literature
Answer Wring
2026 ENGLISH MEDIUM 28 JUNE हिन्दी माध्यम 28 जून
2027 ENGLISH MEDIUM 28 JUNE हिन्दी माध्यम 28 जून
Scan QR code for instant personalized mentoring

1. STATE AND NON-STATE ACTORS

1.1. LEFT-WING EXTREMISM (LWE)

Left Wing Extremism (LWE)

- LWEs are commonly referred to as Maoists globally and as Naxalites within India.
- Naxal insurgency in India originated in the 1967 uprising in Naxalbari, West Bengal.
- Maoist ideology glorifies violence and aims to overthrow the democratic state structure.

Red Corridor	Current Spread of LWE	Achievement in containing
The region affected by LWEs is referred to as Red Corridor in India.	The red corridor has significantly contracted – from over 200 districts in 2005 to just two in 2026.	89% reduction in incidents of LWE violence between 2010 and 2025.

Factors responsible for emergence Of LWE

Jal, Jungle, Jameen (Water, Forest and Land)	Socio-Economic Inequalities	Inadequate implementation of government policies
Expropriation of resources by outsiders, evasion of land ceiling laws	Inequalities in basic services like health, education, roads, and as lack of employment opportunities	Jharkhand is yet to implement Provisions of the Panchayats (Extension to the Scheduled Areas) Act or PESA, 1996

Reasons for decline in LWE Spread in India

Strengthened Security Architecture

- National Policy and Action Plan (2015): Based on the zero-tolerance approach towards Naxalism.
- **SAMADHAN Strategy:** Provides 8 Pillars to tackle LWE (Smart Leadership, Aggressive strategy, Motivation and training, Actionable intelligence, Dashboard based KPIs, Harness technology, Action plan for each theatre, No access to financing)
- **'Modernization of Police Forces' Operation Octopus, Operation Double Bull, etc.**

Developmental

- 178 Eklavya Model Residential Schools functional in LWE-affected districts.
- Special Central Assistance (SCA), Financial Inclusion, Skill & Education, Dharti Aaba Abhiyan

Community Engagement

Civic Action Programme (CAP) to bridge the gaps between Security Forces and local people

Challenges persist in containing LWE

Trust Deficit	Misuse of technology	Difficult Terrain	Security Infrastructure
Cultural differences and perceptions reduce local trust in security and administration	Non-state actors use Dark web to create fake news to malign government, recruit members, virtual currencies for money laundering, etc.	Continuous forest terrain of states like Jharkhand, Chhattisgarh, Orissa	limited intelligence coordination, Easy access to weapons through illegal arms manufacturers, etc.

Way ahead to tackle LWE

Bridging Trust Deficit

- Ensure tribal-friendly land acquisition and rehabilitation policies (Bandyopadhyay Committee).
- Measures like the Forest Rights Act, 2006, should be carefully applied

Countering ideology

Promote constitutional democracy to counter violent Maoist ideology

Security and Capacity building

Focus on modernizing local police and using smart, intel-led units like the Greyhounds for better results

Other

Centre-state coordination, Use of Technology like GIS and GPS

AHMEDABAD | BENGALURU | BHOPAL | CHANDIGARH | DELHI | GUWAHATI | HYDERABAD | JAIPUR | JODHPUR | LUCKNOW | PRAYAGRAJ | PUNE | RANCHI ©Vision IAS

1.2. ARMED FORCES (SPECIAL POWERS) ACT (AFSPA)

Why in the News?

The Ministry of Home Affairs recently extended the Armed Forces (Special Powers) Act, 1958 in parts of **Manipur, Arunachal Pradesh and Nagaland** for another six months.

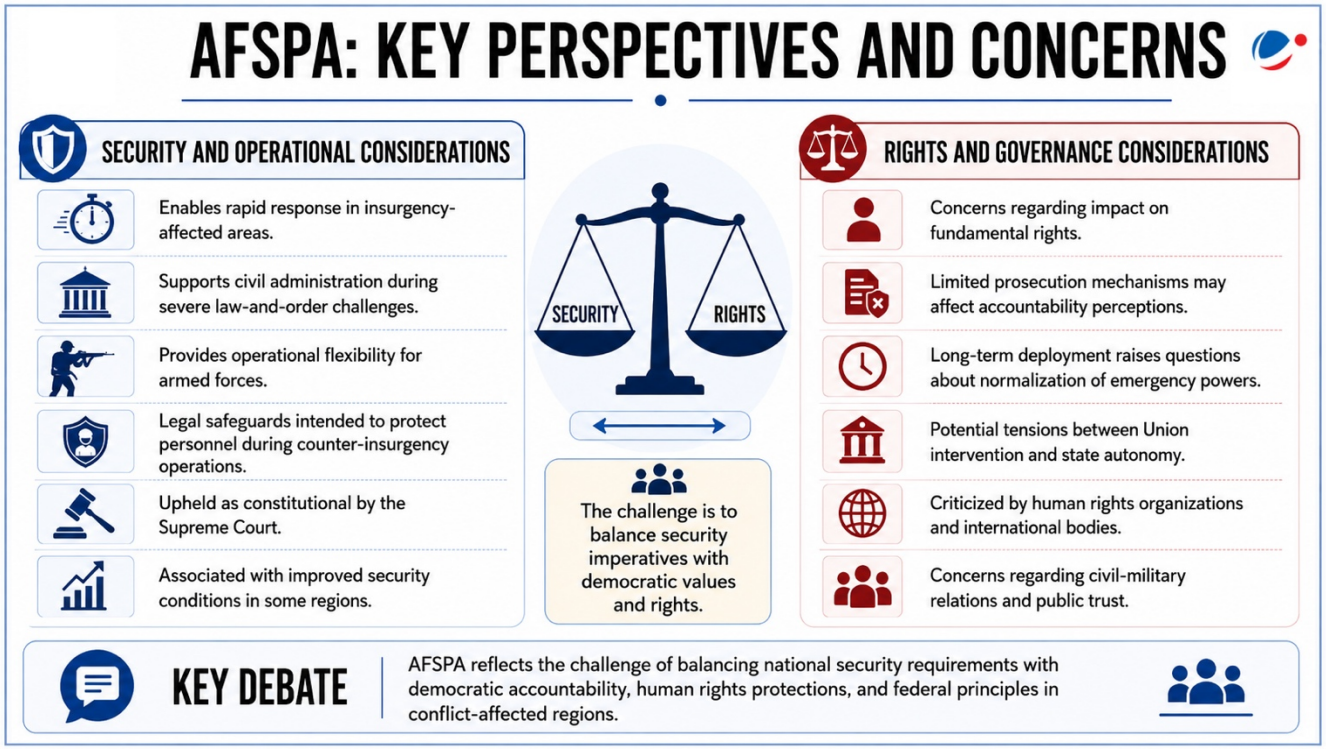
More on the News

About AFSPA, 1958

- It is a special law **granting extraordinary powers to the military** to maintain **law and order.**
- **Objective:** To empower the **armed forces by giving immunity to operate in "disturbed areas"** where **public order is seriously threatened.**
- Currently, AFSPA is in effect in parts of **Nagaland, Assam, Manipur, and Arunachal Pradesh** and J&K.
  - It was lifted from **Tripura in 2015, Meghalaya in 2018 and Mizoram in 1980s.**

Landmark Judicial Decisions

- **Naga People's Movement of Human Rights v. Union of India (1997):** Validated AFSPA constitutionally with safeguards on use of force and immunity.
- **Extra-Judicial Execution Victim Families Association v. Union of India (2016):** Immunity **under Section 6 is not absolute**; accountability **for excessive force is mandatory**.
- **Sebastian M. Hongray v. Union of India (1984):** Security personnel **can be held accountable despite AFSPA immunity.**


AFSPA: KEY PERSPECTIVES AND CONCERNS
SECURITY AND OPERATIONAL CONSIDERATIONS
Enables rapid response in insurgency-affected areas.
Supports civil administration during severe law-and-order challenges.
Provides operational flexibility for armed forces.
Legal safeguards intended to protect personnel during counter-insurgency operations.
Upheld as constitutional by the Supreme Court.
Associated with improved security conditions in some regions.
SECURITY
RIGHTS
The challenge is to balance security imperatives with democratic values and rights.
RIGHTS AND GOVERNANCE CONSIDERATIONS
Concerns regarding impact on fundamental rights.
Limited prosecution mechanisms may affect accountability perceptions.
Long-term deployment raises questions about normalization of emergency powers.
Potential tensions between Union intervention and state autonomy.
Criticized by human rights organizations and international bodies.
Concerns regarding civil-military relations and public trust.
KEY DEBATE
AFSPA reflects the challenge of balancing national security requirements with democratic accountability, human rights protections, and federal principles in conflict-affected regions.

Way Ahead

- **Amend Sections for Accountability:** Amendments may include provisions to prevent extrajudicial killings; present arrested persons before magistrates within 24 hours and limit immunity while establishing oversight for prompt investigations.
- **Alternative Policing**: Use CRPF/state police for **routine law and order; reserve army for high-intensity conflicts.**

- **Human Rights Compliance**: Ensure military operations respect **human rights; strengthen professionalism in counterinsurgency.**
- **Local Trust & Participation**: Involve **civil society, bureaucracy, and army** in local development to **gain public support.**
- **Follow Committee Recommendations:**
  - **Jeevan Reddy Committee (2005)**: Repeal AFSPA; restrict prolonged army deployment; merge powers into Unlawful Activities (Prevention) Act, 1967.
  - **Second ARC (2007):** Repeal AFSPA after **stakeholder consultations.**
  - **Justice J.S. Verma Committee (2013)**: It recommended for **immediate review of AFSPA and if any officer of armed forces commits sexual violence against women** he should be dealt under ordinary criminal law.

Conclusion

AFSPA, while **vital for counterinsurgency** in disturbed areas, **raises concerns over human rights** and **accountability**. A balanced approach **restricting its scope, ensuring oversight, and strengthening local governance** can safeguard security without **compromising democratic values.**

VISIONIAS
INSPIRING INNOVATION
MAINS EDGE 45
Ethics Mains Edge 45
Marks Improvement Classes & Mentoring Programme for UPSC Mains 2026
Smart Answer Writing Intervention for GS Paper 4 (Ethics) under the Guidance of Most Experienced Ethics Faculties of VisionIAS
18 Classes
Intensive Learning
Ethic Theory
Quotes & Case Studies
Offline & Online
Flexible Learning Mode
Scan to Download Ethics Topper Copies
Smriti Ma'am
Jatin Sir
Piyush Sir
https://visionias.in/upsc-mains-edge/
Scan Qr or Visit
18 Workbooks
Structured practice for regular writing discipline.
24h Evaluation
2 answers evaluated daily within 24 hours.
Weekly Mentoring
Direct interaction with expert faculties.
Writing Lab
Vision Answer Writing Lab | 8 AM - 8 PM daily.
Full-Length Test
Comprehensive simulation for exam readiness.
Progress Tracking
Detailed tracking + Hand-written Faculty Notes.
10 June, 11 AM

1.3. INSURGENCY IN NORTH EAST INDIA

Insurgency In India

Insurgency is a violent attempt to oppose a country's government which is carried out by citizens of that country

Reasons behind Insurgency in Northeast India

Large scale **ethnic rivalries** with neighboring tribes. E.g., Meitei vs Kukis in Manipur	Sense of **alienation** from mainstream due to presence of security forces under **AFSPA**	**Territorial Conflicts:** For example, the Assam-Mizoram Border Dispute
Militant group rivalries For example, rivalries in NSCN-Muivah and NSCN-Khaplang factions, complicates Naga talks	**Porous international borders** facilitating arms smuggling and illegal migration	**Lack of effective governance** E.g. Shortage of medical facilities, inadequate housing in Nagaland

Initiatives taken to restore Peace in Northeast

Peace deal/Settlement agreements
- National Liberation Front of Tripura Agreement,
- Bodo Peace Accord,
- Karbi Anglong Peace Agreement.

Strategic Connectivity
- UDAN scheme,
- Rail upgrades (Vande Bharat Express)
- Major bridges/tunnels (Bogibeel, Dhola Sadiya, Metri Setu, Sela Tunnel)

Infrastructure
- India's first National Sports University in Manipur
- AIIMS in Assam
- Aspirational District programme

Cultural Connect
- Inclusion of the Moidams of Choraideo on UNESCO's World Heritage list.
- Ashtalakshmi Mahotsav Northeast's textiles, tourism, GI-tagged products, and crafts

Regional Cooperation
- Shift from "Look East" to "Act East" policy
- Agartala–Akhaura rail link with Bangladesh, and Kaladan Transit,

Way ahead to ensure peace in Northeast India

Political Amend North Eastern Council Act 2002 to restore conflict resolution provision'	**Socio-cultural Connect** Cultural exchanges to raise awareness about Northeast	**De-securitization** Replace border militarization with cross border cooperation
Security: counter-insurgency should be complemented with Peace efforts and human rights protection	**Economic Opportunities** Promote agro-processing, bamboo-based industries	**AFSPA Act** Implement Santosh Hegde Committee (2013) and Justice Verma Committee (2013) recommendations.

1.4. HIGH-POWERED DEMOGRAPHY MISSION

Why in the News?

In his Independence Day address, the Prime Minister announced the launch of a High-Powered Demography Mission aimed at addressing the challenge of illegal immigration.

More on the News

- Illegal immigrants are those who enter the country without valid travel documents in a clandestine and surreptitious manner.
- There is no officially verified estimate regarding the number of illegal immigrants currently residing in India.
  - In 2016, government had informed that there are around 20 million illegal Bangladeshi migrants staying in India.

Factors Facilitating Illegal Immigration/Infiltration into India

Geographical	Socio-Economic	Political/ Administrative	Historical/ Cultural	Security/ Strategic
Porous and **riverine borders** (Bangladesh, Nepal, Myanmar); dense forests and hills, etc.	**Poverty, unemployment, religious persecution,** etc. in neighbouring countries	Corruption (Easy access to forged IDs), political patronage (vote-bank politics), etc.	**Partition (1947) & 1971 war migrations;** shared culture make detection difficult.	**Infiltration by militants** (Pakistan-backed), smuggling networks, poor surveillance infrastructure.

Key concerns associated with Illegal Immigration and Infiltration

National Security Threats

- **Terror Links and Radicalisation: Extremist groups** may **exploit Illegal Immigrant**, such as the Rohingya, for recruitment.
  - India's border also faces threats from **smuggling, human trafficking, and other cross-border criminal activities.**
- **Demographic Shifts and Social Cohesion:** States bordering Bangladesh, such as Assam, have experienced **significant demographic changes** due to the influx of illegal immigrants.
  - Presence of immigrants may lead to **ethnic/religious friction**. **E.g.** Threat to Assamese identity due to illegal migration from Bangladesh.

Socio-Economic Burdens

- **Strain on Public Services/Overburdening of Welfare Schemes**: E.g., healthcare, housing, etc.
- **Distortion in the Labour Market**: **Displacing local workers** and **disrupting wage structures** (often work at lower wages).
- **Other**: Illegal settlers encroach on agricultural and forest lands, etc.

Initiatives taken to Curb Illegal Immigration/ Infiltration in India

- **Legislative and Policy Measures**
  - **Immigration and Foreigners Act, 2025**: Empowers authorities to detect, detain and deport illegal immigrants.
  - **National Register of Citizens (NRC)**: Updated in **Assam** under **Supreme Court** supervision.
  - **Other**: Citizenship (Amendment) Act (CAA), 2019, etc.

- **Border Management Initiatives**
  - **Border Fencing & Floodlighting** (along Indo-Bangladesh and Indo-Pakistan borders)
  - **Comprehensive Integrated Border Management System (CIBMS),** use of smart technologies (radars, sensors, drones)
- **Institutional and Administrative Measures**
  - **Foreigners Tribunals (FTs)**: These are quasi-judicial bodies established through the Foreigners (Tribunals) Order of 1964 under Section 3 of the Foreigners' Act of 1946 to decide cases of illegal immigration and nationality.

Way Forward: Measures to curb Illegal Infiltration/Immigration

- **Security & Intelligence Strengthening: E.g., Integrated Intelligence Grid,** seamless coordination among IB, BSF, state police, and local intelligence units.
- **Strengthen Border Management: E.g.,** Specialized floating Border outpost, UAV monitoring in river stretches, etc.
- **Enacting a National Refugee Law:** India needs a **national refugee law to legally distinguish between genuine refugees and illegal economic migrants**.
  - India is not a signatory to the **1951 UN Refugee Convention** or its 1967 Protocol.
- **Formal Bilateral Repatriation Agreements**: Facilitates the return of their nationals residing illegally.
- **Other**: Expeditiously issue **National Identity Cards (NIDs)**
  - Maintaining Biometric Records of Illegal Immigrants/ Refugees

Conclusion

The High-Powered Demography Mission is a timely step to counter the long-standing challenge of illegal infiltration. Its success will depend on stronger border fencing and surveillance, faster Foreigners Tribunal decisions, bilateral repatriation agreements, and robust national ID systems.

1.5. KEYWORDS

Keywords			
Left Wing Extremism	Red Corridor	Jal-Jangal-Jameen	Socio-Economic Inequalities
Trust Deficit	Constitutional Democracy	Centre-State Coordination	Capacity Building
Alienation	Strategic Connectivity	Cultural Connect	De-securitisation
Disturbed Areas	Immunity	Fundamental Rights	Human Rights
Extra-Judicial Execution	State Autonomy	Accountability	Militarisation of Governance

1.6. PRACTICE QUESTION

Critically examine the factors responsible for the decline of Left-Wing Extremism in India. Do the recent trends indicate its eventual elimination?

Introduction	Body Part: 1	Body Part: 2	Conclusion
Briefly introduce LWE and recent trends.	Factors responsible for decline of LWE.	Challenges hindering complete eradication.	Need for security-development-governance approach.

2. THREATS TO INTERNAL SECURITY

2.1. TECHNOLOGY AND INTERNAL SECURITY

2.1.1. ONLINE RADICALISATION

Online Radicalisation

- **Radicalisation** generally refers to adopting extreme views that may lead to violence or extremist actions.
- **Online radicalisation** is happening due to growing internet access, radical ideas are now easily spread online, making radicalisation faster and harder to control.

Key factors behind radicalisation

Push Factors

- **Economic:** Unemployment, poverty
- **Social:** Marginalization, discrimination
- **Political:** Loss of faith in political institutions

Pull Factors

- **Monetary Incentives**
- **Online Propaganda**
- **Exploiting Crises:** e.g., Israel-Gaza conflict

Factors facilitating online radicalisation

Echo Chamber
Social media creates echo chambers that amplify extremist narratives.

Micro-Targeting & Profiling
Collected user data is used to psychologically influence vulnerable individuals.

Cybercrime as a Tool
Radical groups exploit digital frauds to finance operations and recruit members.

Terror Financing
Online platforms help raise funds through anonymous campaigns.

Challenges in tackling online radicalisation

Easy Digital Access
Growing internet reach increases exposure to extremist content (~**74%** global population is online in **2025**).

Anonymity & Secrecy
Encrypted apps and the Dark Web make detection and tracking difficult.

Psychological Manipulation
Use of gamification and interactive content to lure and indoctrinate youth.

Legal Gaps
No universal definition of radicalisation or terrorism hampers coordination.

Key Initiatives that could facilitate curbing online radicalisation

India

- **Statutory: IT Act 2000** allows blocking harmful content.
- **Institutional: I4C & MeitY** monitor and block URLs threatening national security.
- **Awareness Campaigns: Sahi Raasta** and **Operation SADBHAVANA** by **Indian Army**; **Operation Pigeon** by **Kerala government** to de-radicalize youth.

Global

- **Tech Against Terrorism:** Supports goverments and tech firms in removing terrorist content online.
- **Christchurch Call:** Promotes a safer internet by countering extremist content.
- **INTERPOL:** CBI (as INTERPOL's NCB) leads India's coordination and also launched **Bharatpol** to boost global cooperation.

Way forward to tackle online radicalisation

Build Counter-Narratives
Run awareness campaigns to debunk fake news and break echo chambers.

Strengthen Online Regulation
Enforce content moderation and fact-checking to limit extremist content.

Rehabilitation
Support victims of terrorism through better rights and rehabilitation.

Enhance Global Cooperation
Foster international collaboration between law enforcement and intelligence agencies.

AHMEDABAD | BENGALURU | BHOPAL | CHANDIGARH | DELHI | GUWAHATI | HYDERABAD | JAIPUR | JODHPUR | LUCKNOW | PRAYAGRAJ | PUNE | RANCHI ©Vision IAS

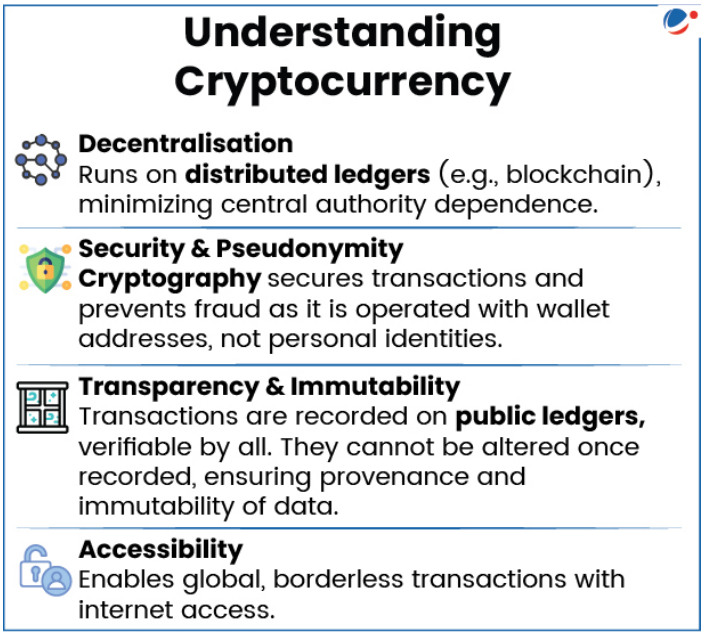
2.1.2. CRYPTOCURRENCIES AND SMUGGLING

Why in the news?

The **'Smuggling in India report 2024-25'** by the **Directorate of Revenue Intelligence (DRI)** highlighted the increasing use of Stablecoins and cryptocurrency for illicit payments of crime particularly in drug and gold smuggling.

About cryptocureencies and Stablecoins

- **Cryptocurrency:** Form of digital currency (based on the blockchain technology) that utilizes a unique software code. E.g., Bitcoin, Ethereum, etc.
  - Blockchain is an **open-source database (public ledger)** distributed across a decentralized computer network/internet that forms a permanent record of transactions between parties.
  - They are **Non fiat** (functions independently of government/Central Bank); have **no intrinsic Value**, etc.
- **Stablecoins:** They are a type of cryptocurrency whose **value is pegged to another asset**, such as a fiat currency or gold, to maintain a stable price.


Understanding Cryptocurrency
Decentralisation
Runs on distributed ledgers (e.g., blockchain), minimizing central authority dependence.
Security & Pseudonymity
Cryptography secures transactions and prevents fraud as it is operated with wallet addresses, not personal identities.
Transparency & Immutability
Transactions are recorded on public ledgers, verifiable by all. They cannot be altered once recorded, ensuring provenance and immutability of data.
Accessibility
Enables global, borderless transactions with internet access.

Reasons for use of Cryptocurrencies/ stablecoins in Smuggling

- **Decentralized:** It allows a **difficult-to-trace environment through dark web marketplaces** for sale of drugs supplied by organized crime syndicates across borders due to its **authorization and borderless nature.**
  - E.g., stable-coins like USDT are increasingly replacing traditional hawala networks.
- **Off-the-book payments:** Crypto wallets, often anonymous and accessible via VPNs, facilitate off-the-book illicit payments, including for **under-invoiced and misdeclared imports** allowing smugglers to evade customs duties and taxes.
- **Pseudonymous nature**: Cryptocurrencies such as Bitcoin allow fraudsters to **conceal their identities**, hindering detection and enforcement.
- **Regulatory Gaps & Jurisdictional Issues**: Law enforcement agencies face significant challenges due to fragmented regulatory landscape, need of advanced **blockchain forensics and authorization of analytical tools** to trace illicit flows.

Regulation of Cryptocurrencies

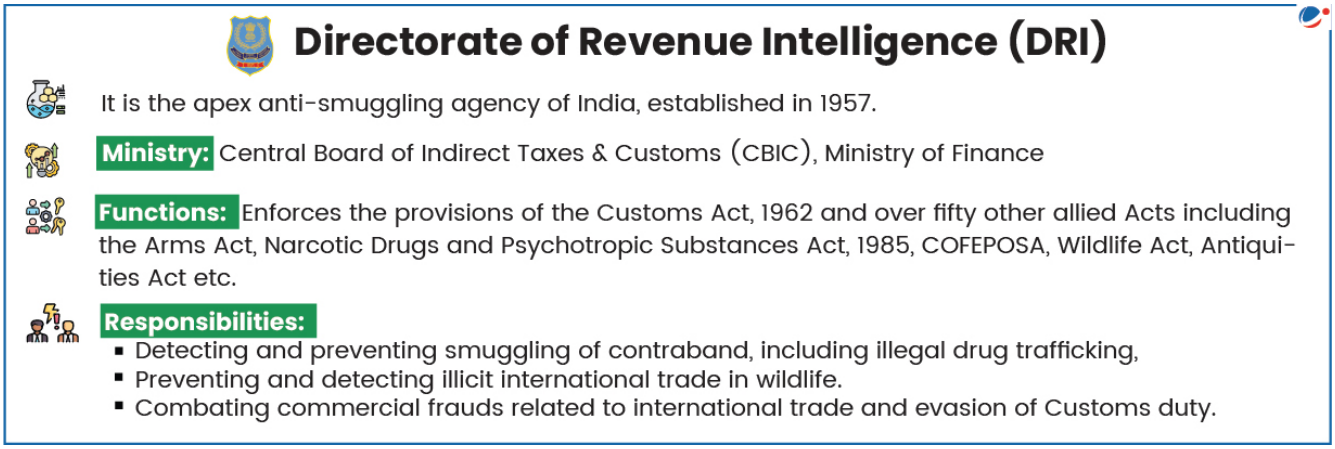
- **India**
  - **Finance Act, 2022: Government** brought a comprehensive taxation regime **for the transfer** of **Virtual Digital Assets (VDAs)** imposing a **30% tax** on **capital gains** from **VDAs.**
    - The **Income Tax Act 1961** defines **VDA** as any information or code or number or token, generated through **cryptographic** means or otherwise; transferred, stored, or traded electronically. E.g. cryptocurrencies, Non-fungible token (NFT), etc.
  - **Prevention and Money-laundering Act, 2002:** In 2023, VDAs were brought under its purview.
- **Globally: Financial Action Task Force (FATF)** to combat illicit finance, the FATF applies international standards for **Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT)** to stablecoins.

Way forward

- **Stronger regulatory frameworks**: E.g., mandating **source-of-funds verification** for all Virtual Digital Asset (VDA) transactions above ₹1 lakh, establishing a **authorization of crypto transaction registry** linked to PAN/Aadhaar etc.
- **Enhanced Anti Money Laundering (AML) compliance**: Integrate VDAs fully into existing AML frameworks to trace illicit proceeds from drug/gold smuggling syndicates.
  - E.g., PMLA enforcement can be strengthened by requiring **mandatory KYC and real-time transaction reporting** from all VDA platforms.
- **Advanced forensic tools**: Develop dedicated blockchain forensics units within DRI and ED, equipped with AI-driven analytics to track authorization of wallet movements, VPN-enabled transactions, and cross-border cryptocurrency flows.
- **Global cooperation**: Negotiate bilateral Multilateral agreements with crypto hubs for intelligence sharing on international syndicates.

Conclusion

The growing use of cryptocurrencies and stablecoins in smuggling reflects how digital anonymity and regulatory gaps are being exploited by 13uthoriza crime networks. Strengthening AML frameworks, blockchain forensics, and international cooperation is essential to curb illicit crypto-enabled trade while safeguarding financial integrity.


Directorate of Revenue Intelligence (DRI)
It is the apex anti-smuggling agency of India, established in 1957.
Ministry: Central Board of Indirect Taxes & Customs (CBIC), Ministry of Finance
Functions: Enforces the provisions of the Customs Act, 1962 and over fifty other allied Acts including the Arms Act, Narcotic Drugs and Psychotropic Substances Act, 1985, COFEPOSA, Wildlife Act, Antiquities Act etc.
Responsibilities:
Detecting and preventing smuggling of contraband, including illegal drug trafficking,
Preventing and detecting illicit international trade in wildlife.
Combating commercial frauds related to international trade and evasion of Customs duty.

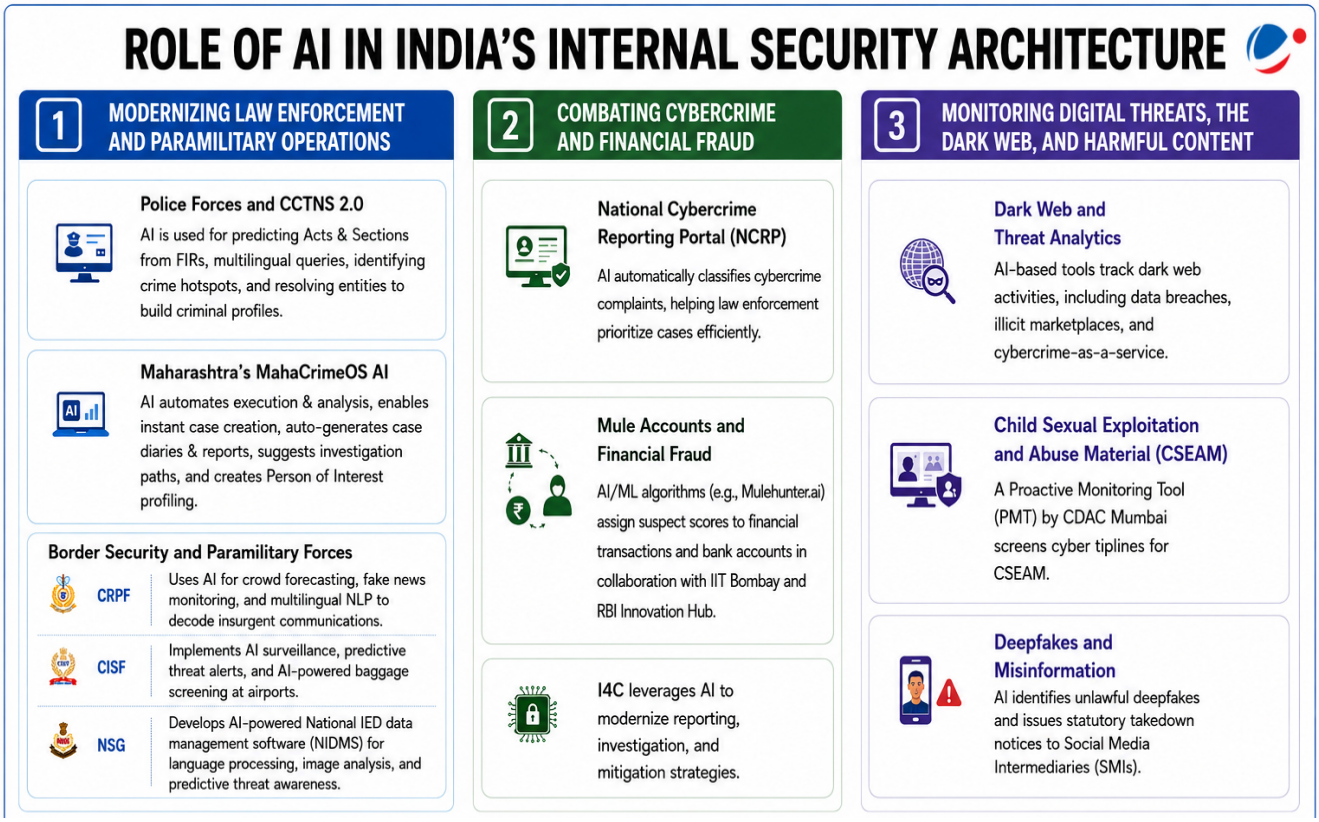
2.1.3. EMERGENCE OF AI IN INDIA'S INTERNAL SECURITY ARCHITECTURE

Why in the News?

The Parliament's **Standing Committee on Communications and Information Technology**, published a report titled **"Impact of Emergence of Artificial Intelligence and Related Issues,"**

More on the news

- The report highlighted the implications of Artificial Intelligence (AI) for India's internal security.
- AI facilitates **real-time surveillance, predictive policing, behavioural analysis, and crime pattern recognition**, enabling faster and more informed decision-making.


ROLE OF AI IN INDIA'S INTERNAL SECURITY ARCHITECTURE
1
MODERNIZING LAW ENFORCEMENT AND PARAMILITARY OPERATIONS
Police Forces and CCTNS 2.0
AI is used for predicting Acts & Sections from FIRs, multilingual queries, identifying crime hotspots, and resolving entities to build criminal profiles.
Maharashtra's MahaCrimeOS AI
AI automates execution & analysis, enables instant case creation, auto-generates case diaries & reports, suggests investigation paths, and creates Person of Interest profiling.
Border Security and Paramilitary Forces
CRPF
Uses AI for crowd forecasting, fake news monitoring, and multilingual NLP to decode insurgent communications.
CISF
Implements AI surveillance, predictive threat alerts, and AI-powered baggage screening at airports.
NSG
Develops AI-powered National IED data management software (NIDMS) for language processing, image analysis, and predictive threat awareness.
2
COMBATING CYBERCRIME AND FINANCIAL FRAUD
National Cybercrime Reporting Portal (NCRP)
AI automatically classifies cybercrime complaints, helping law enforcement prioritize cases efficiently.
Mule Accounts and Financial Fraud
AI/ML algorithms (e.g., Mulehunter.ai) assign suspect scores to financial transactions and bank accounts in collaboration with IIT Bombay and RBI Innovation Hub.
I4C leverages AI to modernize reporting, investigation, and mitigation strategies.
3
MONITORING DIGITAL THREATS, THE DARK WEB, AND HARMFUL CONTENT
Dark Web and Threat Analytics
AI-based tools track dark web activities, including data breaches, illicit marketplaces, and cybercrime-as-a-service.
Child Sexual Exploitation and Abuse Material (CSEAM)
A Proactive Monitoring Tool (PMT) by CDAC Mumbai screens cyber tiplines for CSEAM.
Deepfakes and Misinformation
AI identifies unlawful deepfakes and issues statutory takedown notices to Social Media Intermediaries (SMIs).

Issues associated with AI in law enforcement

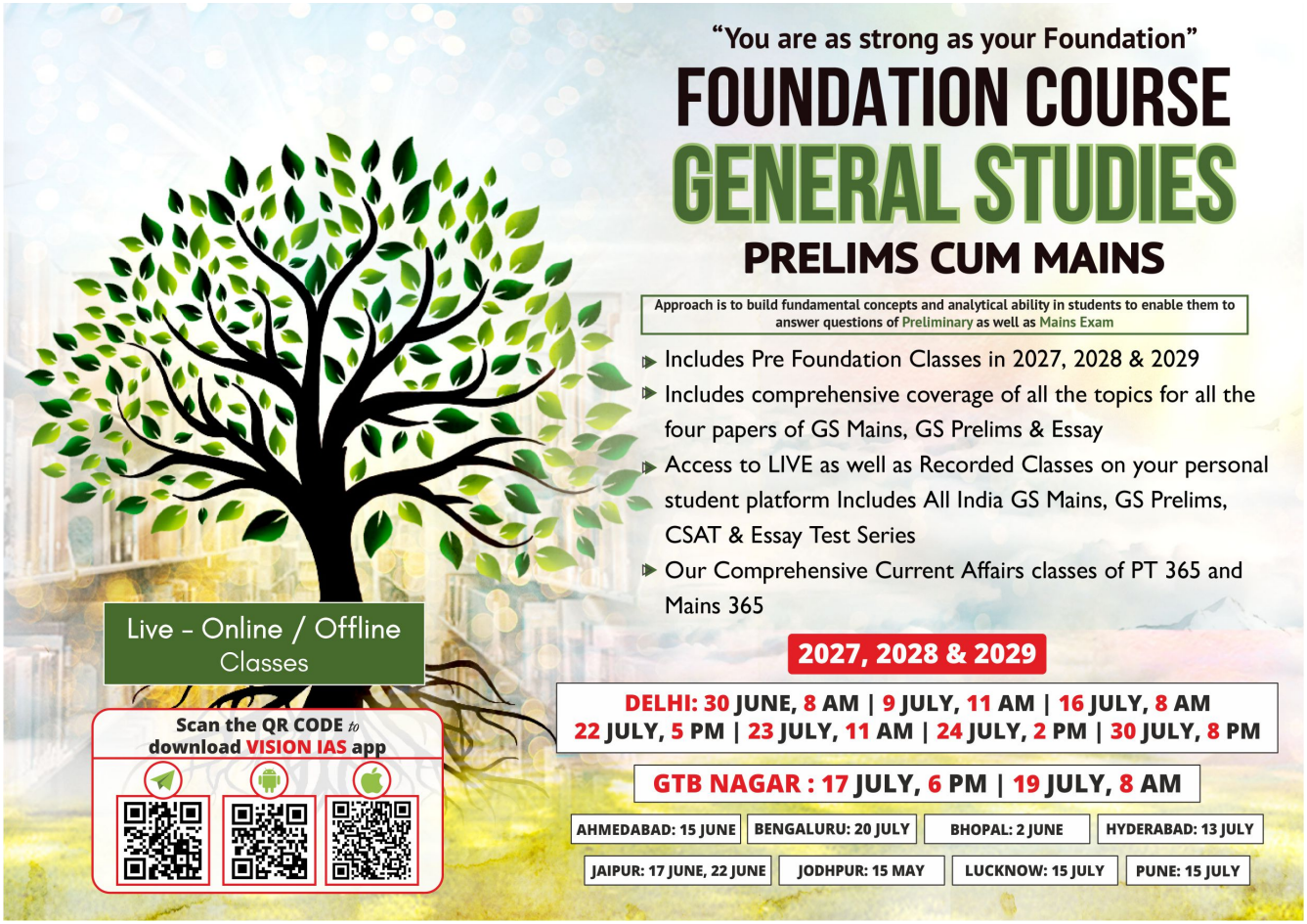
Issue	Key Concern / Example
Privacy & Mass Surveillance	AI-enabled surveillance may infringe privacy and deter free expression. (Puttaswamy Judgment, 2017: Right to Privacy under Article 21).
Algorithmic Bias	AI trained on biased data can reinforce discrimination. E.g. facial recognition systems showing higher error rates for minorities.
Low Transparency	Many AI systems operate as "black boxes," making decisions difficult to explain. E.g. Netherlands' childcare benefits scandal.
Automation Bias	Excessive reliance on AI may undermine human judgment and professional discretion.
Scalability of Errors	Faulty AI systems can rapidly replicate mistakes on a large scale. E.g. Australia's Robodebt scheme issuing incorrect debt notices.
Legal & Governance Challenges	Absence of dedicated AI regulation, concerns over fair trial rights, data security, and accountability.

Way forward

- **Essential Legal and Ethical Guardrails**: Formal statute to govern the **Automated Facial Recognition System (AFRS)** is needed to ensure it does not infringe on constitutional rights to privacy and maintain public trust.
- **Human Rights Impact Assessments**: India should establish a legal framework to conduct **human rights assessments** before any AI system is deployed; ensuring users (agencies) are literate in the system's limitations.
- **Human-in-the-Loop Requirements:** Ensuring that AI risk scores **never become the determinative factor** in arrests or sentencing; human oversight must remain mandatory at every stage.
- **Capacity Building and Knowledge Sharing**: The **National Cyber Crime Research & Innovation Centre (NCR&IC)** along with developing SoPs can train law enforcement personnel in AI adoption effectively.
- **International cooperation:** Invest in international exchange and joint projects and leverage on international organizations such as INTERPOL.

Conclusion

AI cannot serve as an isolated, dependable source for administrative decisions. Governance requires a **hybrid model,** i.e. AI provides data-driven insights, while human administrators provide empathy and moral oversight. For robust implementation, India must enforce regular **algorithmic audits**, maintain a **human-in-the-loop** framework, and strictly implement the **Digital Personal Data Protection Act**.


"You are as strong as your Foundation"
FOUNDATION COURSE
GENERAL STUDIES
PRELIMS CUM MAINS
Approach is to build fundamental concepts and analytical ability in students to enable them to answer questions of Preliminary as well as Mains Exam
Includes Pre Foundation Classes in 2027, 2028 & 2029
Includes comprehensive coverage of all the topics for all the four papers of GS Mains, GS Prelims & Essay
Access to LIVE as well as Recorded Classes on your personal student platform Includes All India GS Mains, GS Prelims, CSAT & Essay Test Series
Our Comprehensive Current Affairs classes of PT 365 and Mains 365
Live - Online / Offline Classes
2027, 2028 & 2029
DELHI: 30 JUNE, 8 AM | 9 JULY, 11 AM | 16 JULY, 8 AM
22 JULY, 5 PM | 23 JULY, 11 AM | 24 JULY, 2 PM | 30 JULY, 8 PM
GTB NAGAR : 17 JULY, 6 PM | 19 JULY, 8 AM
AHMEDABAD: 15 JUNE
BENGALURU: 20 JULY
BHOPAL: 2 JUNE
HYDERABAD: 13 JULY
JAIPUR: 17 JUNE, 22 JUNE
JODHPUR: 15 MAY
LUCKNOW: 15 JULY
PUNE: 15 JULY
Scan the QR CODE to download VISION IAS app

2.1.4. DATA PROTECTION AT A GLANCE

Data Protection in India

- **Data Protection** is the process of safeguarding important data from corruption, compromise or loss.
- **Data** refers to unprocessed facts and figures which could be 'personal' or 'non-personal'.

Relevance of data usage

Political Accountability	Efficient Administration	National security
Can improve transparency in governance by real time monitoring	Helps in making targeted and tailored programmes (E.g. UIDAI)	NATGRID for unified intelligence database and DNA Databanks for both criminal and civil matters

Need for protecting data

Enforcing Right to Privacy	Digitalisation of Economy	Fortify digital governance	Build Public Trust
under Article 21 of the Constitution (Puttaswamy Vs Uol, 20170.	India's digital economy is expected to contribute nearly 1/5th of national income by 2029-30	Quality data powers efficient digital platforms, such as UPI and Aadhaar	Protect Critical infrastructure, prevent cyber financial frauds, etc,

Challenges in data protection

Techno-colonialism	Cyber security Risk	Data Localization Challenges	Other Issues
More than 80% of India's data is exported to global data centers	India Cyber Threat Report 2026 uncovered around 505 detections every minute.	challenges in ensuring secure storage and management of data within India.	Suboptimal funding for research & innovations, low awareness about data privacy, disparities in Digital Literacy, etc.

Steps taken for data protection

Digital Personal Data Protection Act (DPDP), 2023	IT Rules, 2021	Cyber Surakshit Bharat Program	Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA)
Based on BN Sri Krishna Committee, establishes principles for the collection, storage, processing and transfer of personal data.	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 cast specific legal obligations on intermediaries, and platforms to ensure their accountability towards safe and trusted internet.	For enhancing cybersecurity awareness and capacity across the nation.	Launched under the Digital India initiative for promoting Rural Digital Literacy.

Ways to Further Strengthen Data Protection

Enhance Digital sovereignty	Anonymization of personal data	Capacity Building	Learning from Global Best Practices
Build indigenous digital systems e.g., ONDC (Open Network for Digital Commerce), India Stack.	Through techniques like Pseudonymization/ De-identification (e.g. data masking)	Effective Professional Development Programs in Cybersecurity for professionals across Government, Public Sector and Industry launched by the CERT-In.	For example, General Data Protection Regulation (GDPR), Digital Markets Act (DMA) of EU protects the personal data and privacy of people.

2.1.5. CRITICAL INFORMATION INFRASTRUCTURE (CII)

Critical Information Infrastructure (CII)

- The IT Act of 2000 defines "Critical Information Infrastructure" as a "computer resource, the incapacitation or destruction of which shall have debilitating impact on national security, economy, public health or safety".
- It primarily comprises the power, banking, telecom, transport and government sectors.

Threat to Critical Information Infrastructure

State-Sponsored Cyber Attack	IoT Risk	AI in Cybersecurity	Mobile Security Threats
Target critical sectors like energy, banking, telecom; aim for espionage and disruption.	Widespread IoT use in smart grids and smart cities increases exposure.	AI/ML used by both attackers (e.g. automated phishing) and defenders (e.g. threat prediction, incident response).	Mobile devices in CII sectors are targets for malware, spyware and Wi-Fi attacks.

Challenges in Protecting Critical Infrastructure in India

India lacks indigenization in hardware and software cyber security tools like advanced firewall, cloud security etc.	Inhibition in private and public sector to share information about vulnerability of their systems.	Many organizations do not have enough trained security professionals.	Adapting to evolving laws (e.g. Personal Data Protection Bill, IT Act) is challenging.

Steps Taken for Critical Infrastructure protection in India

Legislative measures	Institutional Measures	'Cyber Suraksha' exercise
National Cyber Security Strategy 2020, National Cyber Security Policy, 2013, Information Technology Act, 2000.	National Critical Information Infrastructure Protection Centre (NCIIPC), I4C, CERT-In, National Cyber Coordination Centre (NCCC).	Conducted by Defence Cyber Agency to simulate real-world cyber threats, reinforce secure practices.

Way Forward to Protect Critical Infrastructure in India

Comprehensive Security Approach	Strengthen Cyber Intelligence	Public Private Partnership	Learn from Global Best Practices
Focus on identifying vulnerabilities and interdependencies across sectors.	Adopt modern tools like the Cyber Kill Chain to trace and respond to attack stages effectively.	Sector to enhance research funding and innovation for protection and response mechanisms.	India should formulate international norms for CII protection, inspired by Australia's Critical Infrastructure Resilience Strategy.

2.2. CYBERSECURITY

2.2.1. CYBERCRIME IN INDIA: EVOLUTION, THREATS AND STRATEGIC RESPONSES

Why in the News?

A Parliamentary panel on home affairs presented a report, titled **'Cyber Crime – Ramifications, Protection and Prevention',** highlights the evolution and growing complexity of cyber threats in India.

IMPACT OF RISE IN CYBERCRIME
FINANCIAL LOSSES
India lost over ₹31,500 crore (2019–24) due to cybercrime.
Most crimes are financial in nature (UPI, QR fraud, deepfakes, SIM swaps, etc.).
THREATS TO CRITICAL INFRASTRUCTURE
Multiple agencies have highlighted ransomware attacks targeting Critical Information Infrastructure (CII).
Such attacks aim to paralyse essential services and disrupt national security and public safety.
SOCIAL & PSYCHOLOGICAL IMPACT
Victims of sextortion, cyberstalking, and deepfakes face trauma, social withdrawal, and even suicidal tendencies.
AI-driven deepfakes increasingly target students, hurting mental health and self-esteem.
EROSION OF TRUST
Citizens, especially the elderly, are losing faith in digital services and platforms after repeated frauds and scams.
This erodes confidence in digital transformation and hinders adoption of legitimate online services.
KEY TAKEAWAY:
The rise in cybercrime leads to significant financial losses, threatens critical infrastructure, harms individuals' well-being, and erodes trust in the digital ecosystem.

Current Status

- Cyber threats like **ransomware, AI-driven scams, phishing, and organized financial fraud** are on rise with **internet connections crossing 100 crore in 2025**;
- Protecting Indian **cybersecurity industry, valued at $20 billion** with **400+ startups** and a workforce of **6.5 lakh professionals**, becomes critical.

Contemporary and Emerging Cyber Threats

Quantum-Related Threats

- **Harvest Now, Decrypt Later (HNDL):** Adversaries store encrypted data today for future decryption using quantum computers.
- **Secure Channel Decryption:** Quantum computing could compromise encrypted communications and sensitive networks.
- **Signature Impersonation:** Ability to forge digital signatures and certificates, enabling fraud and malware distribution.
- **Quantum Zero-Day Risks:** Potential discovery of new cryptographic vulnerabilities and challenges in migration to quantum-safe systems.

AI-Related Threats (like Mythos by claude)

- **AI-Driven Vulnerability Discovery:** Advanced AI can identify software weaknesses at scale.
- **Attack Chaining:** Multiple low-risk vulnerabilities can be combined into high-impact cyberattacks.
- **Faster Exploit Development:** AI may accelerate exploit creation faster than organizations can patch systems.
- **Lower Barrier to Cybercrime:** Sophisticated attacks become accessible to less-skilled actors.
- **Critical Infrastructure Risks:** Banking, energy, telecom, and other essential sectors face increased exposure.

REASONS FOR RISE IN CYBERCRIME

RAPID DIGITALIZATION

Expansion of digital platforms like Aadhaar, UPI, DigiLocker and high-speed connectivity has increased the cyber attack surface.

TRANSNATIONAL OPERATIONS

Cross-border scam networks run fraud, extortion and cyber-enabled human trafficking.

CYBERCRIME-AS-A-SERVICE (CAAS)

Ready-made tools and malware on the dark web enable even low-skilled actors to launch sophisticated attacks.

JURISDICTIONAL CHALLENGES

Differences in laws and enforcement across borders provide criminals with safe havens.

EVOLVING CRIMINAL TECHNIQUES

Use of VPNs, encryption, blockchain and decentralised platforms makes detection and tracking increasingly difficult.

LEGAL & CAPACITY GAPS

Legal loopholes, weak accountability, lenient penalties and shortage of cyber experts weaken enforcement.

GOVERNMENT INITIATIVES TO TACKLE CYBERCRIME

Stronger Legal & Regulatory Framework

Cyber offences are covered under the **IT Act, 2000, Bharatiya Nyaya Sanhita (BNS)** crimes, and **Special & Local Laws (SLL).**

Key Provisions of IT Act, 2000

- **Section 69A:** Blocking public access to information
- **Section 79:** Intermediary liability and "safe harbour"
- **Section 70B:** Establishing CERT-In

Agencies & Institutional Mechanisms

- **Indian Cybercrime Coordination Centre, I4C (2020):** National coordination hub; runs **HELPLINE 1930** & National Cybercrime Reporting Portal.
- **CERT-In:** Handles cybersecurity incidents, issues advisories. (EG: ALERTS ON AI-DRIVEN PHISHING). Released Cyber Security Framework and Guidelines for Space including Satellite Communication (SATCOM).
- **National Critical Information Infrastructure Protection Centre (NCIIPC):** Protects Critical Information Infrastructure (power, banking, telecom).
- **CBI & NIA:** Specialised divisions for cyber fraud and terrorism-related crimes. (Eg: Operation Chakra against dark web fraud.)
- **State Initiatives:** Kerala (Cyberdome) and Maharashtra lead in cyber labs & forensics.
- **National Cyber Security Coordinator (NCSC):** Operates under the National Security Council Secretariat (NSCS) to ensure coordination among agencies.
- **Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS):** Toll-free helpline '**1930**' for immediate reporting of financial fraud.

Advanced Technology Tools

- AI/ML for fraud detection (Eg, NPCI's FRM system, RBI's MuleHunter.ai.)
- Deepfake detection tools by MeitY & C-DAC and Cyber Swachhta Kendra to clean malwara & botnets.
- Blockchain & Tokenization: Used by TRAI (spam control) & RBI (card security).

Inter-Agency & International Cooperation

SAHYOG Portal (I4C)
Connects government, intermediaries, and platforms for content takedown and faster coordination.

Collaborations with international agencies and law enforcement bodies to address cross-border cybercrime.

Public Awareness

- Campaigns like **Cyber Dost, RBI Kehta Hai**
- Cyber literacy programs in schools & universities.
- **SEBI's Niveshak Shivir** for investor awareness.

Way forward

- **Empowering CBI**: Parliamentary panel on home affairs recommended amending the Delhi Special Police Establishment (DSPE) Act, 1946, to **empower the CBI to investigate cybercrime cases nationwide without needing general consent from state governments**.
  - This is aimed at overcoming operational delays, as eight states have withdrawn general consent.
- **Legal reforms**: Update the **IT Act** with stricter penalties, a **unified cybercrime law**, and **victim compensation.**
  - Regulate AI-driven content (**deepfakes**), **OTT** platforms **(age-gating, parental controls**), and **online gaming.**
- **Intermediary Accountability**: **Mandate registration of platforms** in India, **appoint local grievance officers,** and ensure **quick takedowns**.
- **Cooperation**: Strengthen State Cybercrime Coordination Centres, create an **international liaison unit**, **a 24×7 cyber desk**, and faster **cross-border** data sharing.
- **Tech Upgrade**: Invest in **AI/ML**-driven threat intelligence**, blockchain** verification**, quantum-resistant encryption,** and an **indigenous** app store.
- **Data Protection**: Align with **DPDP Act 2023 for storage, KYC**, and privacy safeguards.
- **Capacity Building**: **Train police**, prosecutors, judiciary, and students in cybersecurity; expand **forensic labs and VR-based training**.
- **Public Awareness**: Run **multilingual** awareness campaigns**, financial literacy** drives and regulate **finfluencers.**

2.2.2. DIGITAL SOVEREIGNTY

Digital Sovereignty

- **Digital Sovereignty** is the authority of a nation to govern its own digital space, infrastructure and data flows, ensuring they align with national laws, security interests and cultural values.

- This concept operates across three distinct layers:
  - **Physical Layer:** Control over infrastructure and technology.
  - **Code Layer:** Authority over standards, rules and design.
  - **Data Layer:** Ownership of data flows and usage.

Need of Digital Sovereignty

Economic Advantage: AI is projected to generate trillions of dollars in economic dividends and productivity gains, currently benefitting Global North at the expense of Global South.

Strategic Autonomy: AI is becoming a pillar of economic and military power. Countries don't want to be dependent on the US or China for foundational AI models and computing power.

Cultural Preservation: Sovereign foundation models, such as Large Language models (LLMs), can be trained on local datasets (e.g. dialects, societal practices) to promote inclusiveness and revitalize indigenous languages.

Data Sovereignty: To ensure critical data (citizens' data, defense, infrastructure, healthcare) stays within national control and is not processed by foreign tech giants. E.g. US based models such as ChatGPT, Grok, etc.

Fostering Innovation: Reducing reliance on foreign hyperscalers creates space for a domestic cloud ecosystem, generating up to 2 million jobs by 2030.

Challenges to make India as digitally Sovereign

Global Digital Dominance: Dependence on foreign-controlled digital and financial ecosystems limits strategic autonomy.

Digital Trade Pressures: International trade agreements may constrain India's policy space and data governance choices inducing digital capitulation.
Digital capitulation involves trading away digital autonomy for immediate commercial gains.

Technology Dependence: India imports over 95% of its semiconductors and foreign hyperscale's like AWS, Azure, and Google dominate 90% of the Indian market for cloud storage.

Infrastructure Gap: While India generates 20% of the world's data, it possesses only 2-3% of global data center capacity.

Legal Vulnerability: Data hosted by foreign providers may remain subject to overseas laws and regulations.

Steps taken to promote Digital Sovereignty in India

Digital Personal Data Protection Act, 2023: Promotes digital sovereignty by asserting control over how the personal data of Indian residents is handled, both within and outside the country.

Sectoral Localization: Reserve Bank of India (RBI) in 2018 directed all payment system providers to ensure that "the entire data relating to payment systems operated by them" be stored in systems located only in India.

Government Cloud Initiatives: The government launched "Meghraj" (GI Cloud)"to accelerate the delivery of e-services and ensure government data is hosted on sovereign infrastructure.

Judicial Intervention: The Supreme Court's Puttaswamy judgment (2017) declared privacy a fundamental right, reinforcing the India's obligation to protect citizen data from unauthorized foreign or domestic surveillance.

Others: Sovereign AI (E.g., BharatGen); Free and Open-Source Software (FOSS) approach, Indigenous Technology (E.g., Arattai, messaging app developed by Zoho), etc.

Pathways for Digital Sovereignty in India

Sovereign-First for Critical Infrastructure: India should mandate that all "Critical" or "Senstive" data (e.g., defence, health, bulk citizen data) be hosted on Indian-domiciled sovereign clouds.

Resisting "Digital Self-Sabotage": India must resist FTA clauses that prevent discrimination against foreign digital services, as agreeing to them would amount to "digital self-sabotage" and halt the growth of indigenous capabilities.

Sovereign AI: Subsidize "compute credits" for researchers and startups to use domestic Graphics Processing Unit (GPU) clouds (like Yotta's Shakti Cloud) to build indigenous AI models.

From Service to Ownership: India must pivot from merely exporting software services (currently valued at $224 billion) to creating "sovereign data capital" and proprietary AI.

Digital Industrialization: Unlike China's exclusion model (restricting foreign Big Tech to nurture giants), India should develop a national digital industrialization policy framework.

2.2.3. UNITED NATIONS CONVENTION AGAINST CYBERCRIME

Why in the News?

Recently, 72 of the 193 member states signed the United Nations Convention against Cybercrime in Hanoi, Vietnam.

About United Nations Convention Against Cybercrime

- **Convention** was **adopted by the General Assembly** of the United Nations on 24 December 2024.
- It will enter into force **90 days after the 40th State deposits its ratification**.
  - The signing process will remain **open until 31 December 2026**.
  - **India has not signed the treaty yet**.
- **UN Office on Drugs and Crime (UNODC)** served as secretariat to negotiations.
- **UN Convention Against Cybercrime** is the **first universal legally binding framework** for the collection, sharing and use of electronic evidence for all serious offences.
  - **Budapest Convention on Cybercrime (2001),** drafted by the Council of Europe**, was the first international treaty** focused on combating cybercrime and strengthening cross-border cooperation.
  - A number of states such as Russia and China have rejected the Budapest Convention and have long advocated for a new international cybercrime convention.

Key features of the Convention Against Cybercrime

- **Expanded Scope of Cyber Offences:** It criminalize cyber-dependent crimes and also **offences related to online fraud, online child sexual abuse**, **non-consensual dissemination of intimate images etc.**
- **International Cooperation**: It establishes a 24/7 network to boost international cooperation.
- **Protection of sovereignty:** States Parties shall carry out their obligations under this Convention in a **manner consistent with the principles of sovereign equality and territorial integrity of States** and that of non-intervention in the domestic affairs of other States.
- **Victim Support:** The Convention encourages States to provide victims with **access to recovery services, compensation, restitution and the removal of illicit content.** This support will be delivered according to each country's domestic laws.
- **Respect for human rights**: States Parties to ensure that the implementation of their obligations under the Convention is consistent under **international human rights law.**

Significance of the Convention

- **Relevance of Multilateralism:** The convention marks the **victory of multilateralism**, reflecting collective will of States to promote international cooperation for combating cybercrime.
- **Tackle Rising Digital Threats:** Global cybercrime costs are projected to **reach $10.5 trillion annually by 2025**, as per industrial experts.
- **Helping Global South States:** Global convention would help developing countries who often lack **robust cybersecurity infrastructure.**
- **Emerging Challenges:** It provides a cooperative framework to address new and evolving threats such as AI-driven cyberattacks, deepfakes, disinformation campaigns etc.

2.2.4. QUANTUM CYBER READINESS

Why in the News?

MeitY, CERT-In and cybersecurity firm SISA jointly launched a whitepaper titled "**Transitioning to Quantum Cyber Readiness**" to prepare for disruptive potential of quantum technologies, especially in cybersecurity.

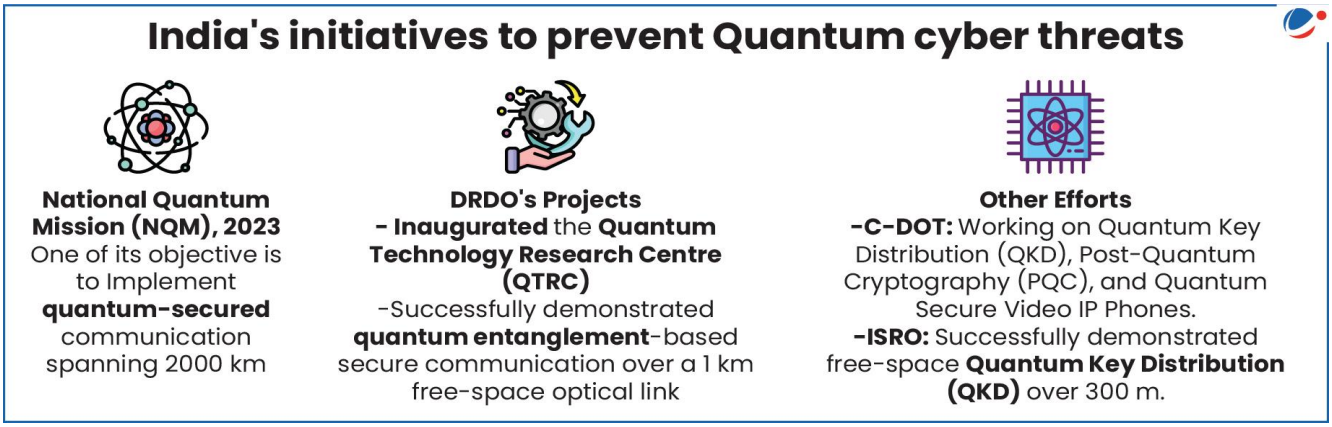
More on the news

- The whitepaper warned that Quantum computers pose a **serious threat to current encryption algorithms** by breaking asymmetric cryptographic protocols such as Rivest-Shamir-Adleman (RSA).

- Quantum computers can solve **complex, intractable mathematical problems** - and perform tasks in machine learning, optimization and logistics - orders of magnitude faster than conventional computers.
- As per the paper, **any data requiring protection beyond 2030** should be considered at immediate risk.

Cyber Threats related to Quantum Technology

- **Harvest Now, Decrypt Later (HNDL) Attacks:** These attacks **involve adversaries** collecting and storing encrypted data today with the intention of decrypting it once quantum computers become capable of breaking current cryptographic systems.
- **Secure channel decryption:** Quantum computing can break encrypted network communications and **"listen in"** on sensitive conversations like defence communications.
- **Signature impersonation:** Quantum computing can enable attackers to forge digital certificates, enabling malware distribution and targeted phishing.
- **New "Zero-Day" vulnerabilities:** This includes the potential for yet unknown quantum algorithms to break existing cryptographic systems and challenges associated with transitioning to quantum-resistant cryptography.


India's initiatives to prevent Quantum cyber threats
National Quantum Mission (NQM), 2023
One of its objective is to Implement quantum-secured communication spanning 2000 km
DRDO's Projects
- Inaugurated the Quantum Technology Research Centre (QTRC)
-Successfully demonstrated quantum entanglement-based secure communication over a 1 km free-space optical link
Other Efforts
-C-DOT: Working on Quantum Key Distribution (QKD), Post-Quantum Cryptography (PQC), and Quantum Secure Video IP Phones.
-ISRO: Successfully demonstrated free-space Quantum Key Distribution (QKD) over 300 m.

Way Forward: Roadmap for Quantum Cyber Readiness recommended by whitepaper

Area	Key Recommendations
Assessment & Planning	Develop a Quantum Bill of Materials (QBOM) for risk mapping and compliance. Use AI-driven risk assessment to identify cryptographic vulnerabilities.
Technology Readiness	Test and validate Post-Quantum Cryptography (PQC) before deployment. Adopt Hybrid Cryptography combining classical and quantum-resistant algorithms.
Organizational Rollout	Integrate PQC into software development and key management workflows. Update ICT and security policies to mandate approved PQC standards.
Resilience & Futureproofing	Explore Quantum Key Distribution (QKD) for enhanced security. Use ML-DSA (Module Lattice-based Digital Signature Algorithm) and SLH-DSA (Stateless Hash-based Digital Signature Algorithm) for high-security digital signatures and critical transactions.

Conclusion

The quantum revolution is inevitable, but organizations that act decisively and strategically will not only protect their data from quantum risks but also lead the way in shaping a quantum-resilient future.

2.3. TERRORISM

Terrorism In India

India ranked 13th on Global Terrorism Index 2026 (Topped by Pakistan).

Challenges to counter International Terrorism

Definition Gap	State Sponsored	Ineffective global cooperation	Global Radical Ideologies	Anonymity in Terror Financing
No global consensus on definition of 'terrorism'.	Pakistan has supported terrorism through funding, logistics, materials, and training (2025 FATF report).	E.g. Extradition reupests for high-profile terrorists like Tahawwur Hussain Rana faced delays	Influence of extremist groups like ISIS spread through transnational networks.	Terror groups use social media, crowdfunding, Bitcoin, and even online gaming to raise and transfer funds secretly.

Counter terrorism Initiatives

India

- **New Security Doctrine (2025):** Zero tolerance for terrorists and their supporter
- **UAPA, 1967:** Legal framework to ban terrorist activities.
- **NIA:** Central agency to investigate terror cases.
- **NATGRID:** Database for real-time intelligence sharing.
- **New MHA Divisions:** Counterterrorism & Counter-Radicalisation Division; Cyber & Security Division
- **PRAHAAR:** Seven pillared National Counter-Terrorism Policy & Strategy.

Global

- **Financial Action Task Force (FATF):** Apex watchdog for Anti-Money Launderring and Countering the Financing of Terrorism.
- **UN Global Counter-Terrorism Strategy (2006):** Boosts global cooperation against terrorism.
- **UNSC Counter-Terrorism Committee (CTC):** Ensures countries follow anti-terror Resolution 1373 (2001).
- **Global Counterterrorism Forum (GCTF):** Multilateral anti-terror platform; India is a member.
- **SCO RATS:** Fights terrorism, extremism, and separatism in the region.
- **No Money for Terror Conference:** India hosted the 3rd conference in New Delhi to combat terror financing.

Way Ahead for tackling terrorism

Define Terrorism	Institutional Reforms	Strengthen Global Cooperation
adoption of Comprehensive Convention on International Terrorism (CCIT) at the UN proposed by India in 1996.	Transparency in decision making of global watchdogs like reason for removing Pakistan from grey list of FATF is needed.	Cooperate with regional/international bodies; follow global norms like UNSC Delhi Declaration on tech misuse by terrorists.

2.3.1. STATE-SPONSORED TERRORISM

Why in the news?

The Financial Action Task Force (FATF) report "Comprehensive Update on Terrorist Financing Risks" included a separate section on state-sponsored terrorism in its report for the first time.

About State-Sponsored Terrorism

- It means a **government actively supporting, either directly or indirectly, violent non-state actors** in carrying out acts of terrorism.
- **Report findings on State-Sponsored Terrorism:**
  - It remains **a persistent threat** to global peace, security and regional financial and political stability.
  - Highlights the funding patterns of **Pakistan-based LeT (Lashkar-e-Taiba) and JeM (Jaish-e-Mohammed)**
    - This **reinforces India's position identifying Pakistan as a high-risk Terror Financing (TF)** source in its National Risk Assessment for Money Laundering and Terrorist Financing (NRA) 2022.

Implications of State-Sponsored Terrorism for India

- **Pakistan provides Safe Havens:** to terrorist organizations like Al Qaeda, Lashkar-e-Taiba, Jamat-Ud-Daawa, JeM etc. to fulfil its political agenda.
- **Human Costs and Trauma:** Eg. Mumbai and Pahalgam terrorist attacks.
- **Politicisation of the UN Sanctions Committees:** Eg. China often puts holds and blocks on proposals to blacklist Pakistan-based terrorists at the UN (as seen in the case of Masood Azhar).
- **Campaigns of misinformation and disinformation:** Eg. By Pakistan in Kashmir.

Efforts by India to voice its concerns globally

- **Comprehensive Convention On International Terrorism (CCIT)**: It is India's proposed policy for zero tolerance against terrorism in all its forms.
- **Co-sponsored the UN General Assembly resolution** on 'Enhancement of international cooperation to assist victims of terrorism.
  - **India also** supports **establishment of a voluntary fund** aimed at strengthening Member States' efforts in assisting victims of terrorism through national systems.
- **Global Counter Terrorism Strategy (GCTS):** India has contributed **constructively to strengthen the language of provisions** related to victims of terrorism.
- **Dialogue on Counter Terrorism**: India engages **bilaterally with Australia, Canada, Egypt, etc** and **multilaterally at ASEAN, BIMSTEC, BRICS** to establish Joint Working Group to counter terrorism.

Way Forward (FATF report)

- **Strengthening regulatory frameworks** for emerging sectors such as virtual assets and social media platforms.
- **Fostering and Strengthening international cooperation**, targeted public-private partnerships, and using practical risk indicators—like payment patterns, travel, and social media activity—to detect and curb terrorist financing.
- **Continued monitoring** of both traditional and new methods to ensure the regulatory response keeps pace.

Conclusion

To strengthen our collective understanding of Terrorist Financing risks, sustained efforts will be needed in the coming years, including regularly updated national, supranational, sectoral, and emerging risk assessments.

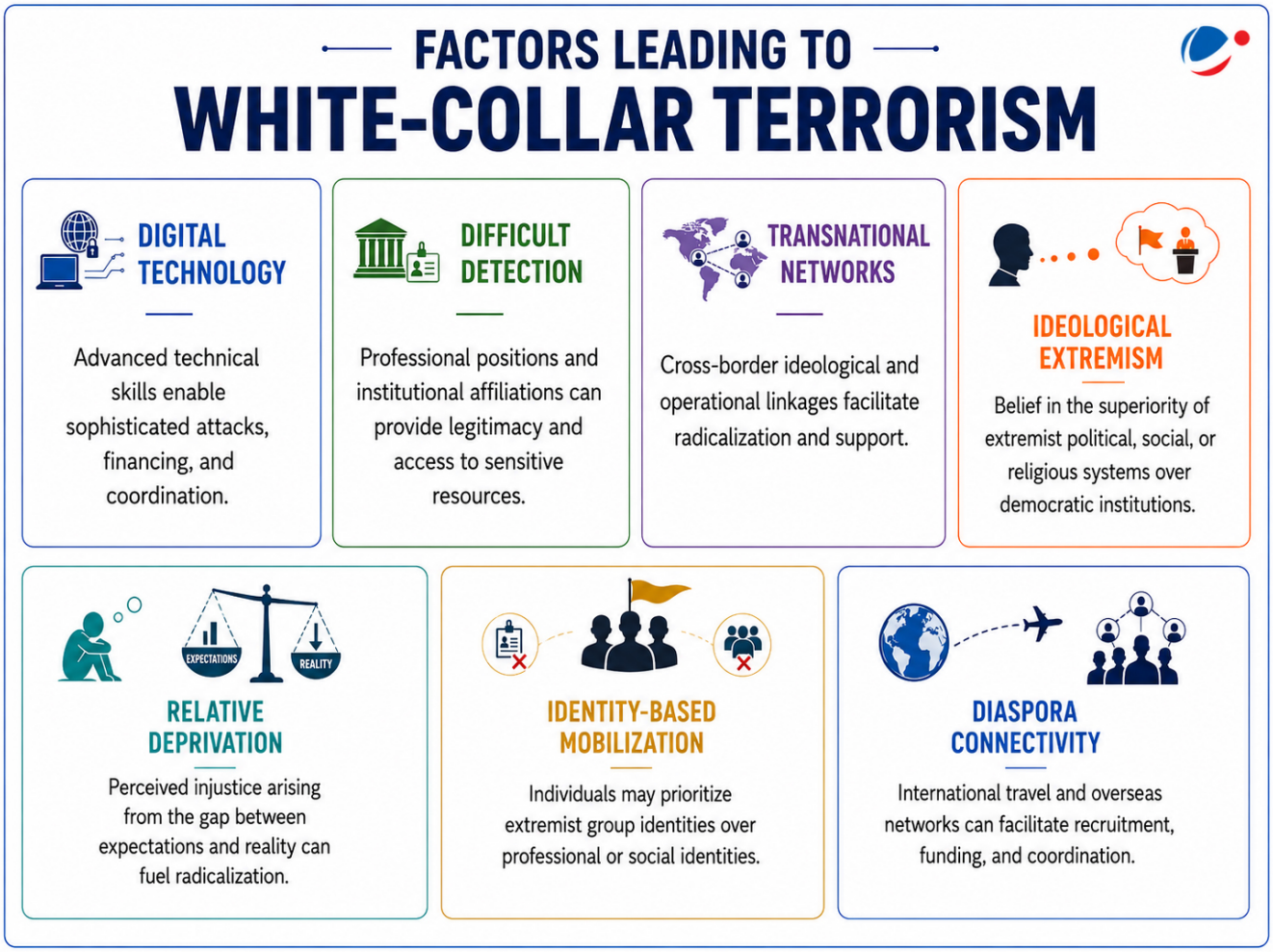
2.3.2. WHITE COLLAR TERRORISM

Why in the News?

The National Investigation Agency (NIA) has arrested Doctor from Baramulla, J&K, as the eighth key accused in the last month's Delhi bomb blast case described as an act of White-Collar Terrorism.

About White Collar Terrorism (WCT)

- **Genesis**: The concept derives **its origin from Edwin Sutherland concept of "White-Collar Crime"** which shifts focus to crimes by respected professionals in the society.
- **Definition**: It refers to the **covert participation of professionals** in enabling, designing, financing, or shielding terrorist operations.
  - These individuals **weaponise intellect** rather than arms, crafting encrypted communication systems, laundering funds across borders, forging identities, exploiting bureaucratic loopholes, or leaking classified information.
  - There is currently **transition from the role of intellectuals as facilitators to direct participation** in the acts of terror as seen in the Delhi Blast case.
- **Evolution of White-Collar Terrorism**: In 1980s, White-collar professionals raised funds for violent organizations such as Palestinian Liberation Organization (PLO) and the Irish Republican Army (IRA) in North America.
  - The Engineers in ISIS's weapons program, doctors in AlQaeda's networks and IT specialists who created sophisticated propaganda machinery.
  - **India**: The entire group of ISIS recruits from **Kerala** came from **well-to-do upper-middle-class** families with sound educational background.
- **How it is different from Traditional Terrorism:**
  - Unlike **traditional terrorism, which relies on overt violence and intimidation**, WCT operates through **subversion and enablement**. Its motivation is ideological, religious, or political, which distinctly separates it from **white-collar crime, which is solely motivated by financial gain**.
  - It thrives on deception, legitimacy and their privileged access to sensitive structures.


FACTORS LEADING TO
WHITE-COLLAR TERRORISM
DIGITAL TECHNOLOGY
Advanced technical skills enable sophisticated attacks, financing, and coordination.
DIFFICULT DETECTION
Professional positions and institutional affiliations can provide legitimacy and access to sensitive resources.
TRANSNATIONAL NETWORKS
Cross-border ideological and operational linkages facilitate radicalization and support.
IDEOLOGICAL EXTREMISM
Belief in the superiority of extremist political, social, or religious systems over democratic institutions.
EXPECTATIONS
REALITY
RELATIVE DEPRIVATION
Perceived injustice arising from the gap between expectations and reality can fuel radicalization.
IDENTITY-BASED MOBILIZATION
Individuals may prioritize extremist group identities over professional or social identities.
DIASPORA CONNECTIVITY
International travel and overseas networks can facilitate recruitment, funding, and coordination.

Way Forward

- **Stronger Regulation & Enforcement**: Tighten NGO audits, compliance and blacklisting; empower ED/CBI to probe financial links to WCT.
- **Enhanced Institutional Oversight**: Enforce background checks, forensic audits and security officers in universities; digitally track sensitive materials.
- **Global Transparency Alignment**: Adopting FATF aligned reporting to close funding and oversight gaps.
- **Crack Down on Laundering Networks**: Strengthen KYC with biometrics; monitor high-value transactions and shell entities via FIU-India and ED.
- **Fiscal Transparency & Accountability**: Promote citizen led budget monitoring to curb corruption and misuse of public funds.
- **Unified Risk Intelligence Grid**: Create a national registry of sensitive professions linking IB, NIA, ED and state police databases.
- **Early Radicalisation Warning**: Train educators and managers to identify red flags; enable anonymous reporting and prevention programs.

Conclusion

White collar terrorism is, ultimately, the **new face of extremism**, **quiet, intelligent, and embedded within society** itself. In India's case, it is not an anomaly but **an emerging pattern**, one that requires urgent recognition and strategic countermeasures. The threat no longer comes only from the shadows of conflict zones; it now emerges from classrooms, clinics, offices, and research labs. And that is what makes it far more formidable.

Lakshya
MAINS MENTORING PROGRAM 2026
50 Days Expert Intervention
A Strategic Revision, Practice, and Mentoring Program for UPSC Prelims Examination
16 JUNE 2026
Highly experienced and qualified team of Mentors for continuous support and guidance
A structured plan of revision for GS Prelims, CSAT, and Current Affairs
Effective Utilization of learning resources, including PYQs, Quick Revision Modules (QRMs), and PT-365

Lakshya
PRELIMS & MAINS INTEGRATED MENTORING PROGRAM
Lakshya Prelims & Mains Integrated Mentoring Program 2027
(A Strategic Revision, Practice, and Mentoring Program for UPSC Prelims and Mains Examination 2026)
VisionIAS introduces the Lakshya Prelims & Mains Integrated Mentoring Programme 2027, offering unified guidance for UPSC aspirants across both stages, ensuring comprehensive support and strategic preparation for success
2027
14 MONTHS
1 JULY
Highlights of the Program
Coverage of the entire UPSC Prelims and Mains Syllabus
Development of Advanced answer writing skills
Highly experienced and qualified team of senior mentors
Special emphasis to Essay & Ethics

2.4. TRANSNATIONAL ORGANIZED CRIMES (TNOCS)

Transnational Organized Crimes (TNOCs)

- **Organized crimes** are illegal activities, conducted by groups or networks acting in concert for a financial or material benefit
- **Transnational Organized Crimes (TNOCs)** operates across borders, exploiting vulnerable people and undermining global security.

Types of TNOC

Drug trafficking	**Human trafficking**	**Smuggling of migrants**	**Money laundering**	**Illicit trading in firearms**
Crimes that affect the environment			**Cybercrime**	

Challenges in curbing TNOCs

Cross-Border Complexity
TNOCs span multiple countries, making law enforcement and jurisdiction difficult.

Legal and Policy Gaps
Different laws and systems across countries hinder coordinated global action.

Demographic Winter
Ageing populations in developed countries increase demand for labour and fuels trafficking.

Economic Inequality
Poverty and joblessness drive vulnerable individuals toward organized crime networks.

Steps taken to address TNOCs

National

- **Constitutional and Statutory Framework:** Article 23 of the Constitution and Immoral Trafficking Prevention Act, 1956 prohibit human trafficking.
- **Maritime Security:** In 2022, India joined Combined Maritime Forces to fight illegal activities by non-state actors at sea.
- **National Central Bureau (NCB):** CBI acts as India's National Central Bureau for INTERPOL coordination.

Global

- **UN Conventions:** UNTOC and its protocol against migrant smuggling (ratified by India) promote international cooperation.
- **UN Commission on Crime Prevention and Criminal Justice (CCPCJ):** Main UN body for crime prevention and justice policies.
- **FATF:** Apex watchdog for Anti-Money Laundering and Countering the Financing of Terrorism.
- **INTERPOL:** INTERPOL's Organized Crime Unit and Project Millennium support tracking global crime networks.

Way Forward to Tackle TNOC

Secure Financial Systems
Protect markets and banking systems from criminal networks.

Enhance Law Enforcement
Provide specialized training and boost intelligence capabilities.

Increase Accountability
Launch global initiatives to hold countries accountable for enabling organized crime.

Focus on Rehabilitation
Reduce repeat offences through rehabilitation and reintegration of offenders.

2.5. MONEY LAUNDERING AND SMUGGLING

Money Laundering in India

Money Laundering is the process of making illegally-gained proceeds appear legal. Money could be laundered through hawala, cryptocurrencies, shell companies, bulk cash smuggling, etc.

Three stages of Money Laundering

Placement	Layering	Integration
Illegal money is introduced into legal and financial systems	Carrying out multiple complex transactions to create confusion and make it challenging to trace money back to its illegal origins	Laundered funds are integrated back into legitimate economy, appearing as clean and lawful money

Consequences of money laundering

Security threat	Economic threat	Social threat	Governance threat
Such money is used for arms dealing, organized crime, terrorist financing, drug and sex trafficking, etc.	Loss of revenue to the government, policy distortion occurs because of measurement error, Loss of confidence in markets, etc.	May fuel illegal activities like drug addiction, rampant corruption.	Less money for development schemes, increase compliance costs, and exacerbate social inequality.

Challenges in curbing Money Laundering

Weak enforcement mechanism	Delay in Prosecution:	Virtual Digital Assets (VDAs)	Other
ED secured convictions in just **4.6%** in **PMLA** cases in last **5** years	Prevalence of delays relating to concluding money laundering and terrorist financing prosecutions highlighted by **FATF**.	They provide anonymity and bypassing traditional financial oversight.	Lack of necessary political will, Tax haven countries, Poor Inter-Agency

Initiatives to prevent money laundering

Statutory Measures	Institutional framework:	Taxing VDA	Global
Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, **2015 (BMA, 2015)** Prevention of Money Laundering Act, **2002 (PMLA)**,	Directorate of Enforcement **(ED)** and Financial Intelligence Unit – India **(FIU-IND)**.	Even tough in India crypto-assets are not legal tender, income from VDAs like cryptocurrencies is taxed at **30%** and a **1% TDS** is applied on crypto transactions to monitor and track usage.	• Financial Action Task Force **(FATF)** • UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances **(Vienna Convention)**, • Global Programme against Money Laundering.

Way Forward to Counter Money Laundering

Stronger Due Diligence	Use of Advanced Technologies	Better Coordination	Global Cooperation
Flag and report suspicious transactions to the Financial Intelligence Unit **(FIU)** for timely action.	Adopt **AI** and **Blockchain** to improve efficiency and trace transactions.	Ensure regular communication and data sharing between banks and law enforcement.	Support international efforts like the **Palermo Convention (2000)** and **UN Convention Against Corruption (2003)** to fight cross-border financial crimes.

2.5.1. DRUG TRAFFICKING

Drug Trafficking in India

Drug Trafficking is the illegal production, distribution, and sale of substances banned under drug laws. 316 million people used drugs in 2023 — a 28.5% increase in 10 years (World Drug Report 2025).

Key Issues Linked to Drug Trafficking

National Security Threat
- Fuels crimes like human trafficking and money laundering
- Leads to narco-terrorism, destabilising regions
- Drug money funds terrorism and LWE

Rising Social Crimes
Increases youth addiction, affecting public health and law & order

Institutional Corruption
Drug cartels infiltrate and corrupt state systems
E.G., PUNJAB DRUG SCANDAL 2024

Environmental Damage
Illegal drug farming causes deforestation and increases carbon footprint
E.g., Cannabis cultivation in Uttarakhand

Key challenges in tackling drug trafficking in India (INCB Report 2023)

Transit Hub
India is wedged between the world's two largest areas of illicit opium production, Death/ Golden triangle (Myanmar, Thailand and Laos) and Death/Golden Crescent (Afghanistan, Iran and Pakistan).

Cyber enabled trafficking
Cyber-enabled drug markets, operating on the dark web and crypto-markets, are making illicit drugs more accessible than ever before

illegal online pharmacies
Proliferation of illegal online pharmacies poses a significant challenge to drug control efforts.

Measure taken by India to tackle drug trafficking

Statutory
- Narcotics Drugs and Psychotropic Substances Act, 1985.
- NIA empowered for narco-terrorism since 2020

Databases
SIMS and NIDAAN (National Integrated Database on Arrested Narco-offenders) portals for drug offences/offenders

Task Forces
Anti-Narcotics Task Forces (ANTF) in states/UTs

Global Cooperation
- UN Single Convention on Narcotics Drugs 1961
- UN Convention against Corruption (UNCAC) and UNTOC

Way Forward

Accountability
Create accountability rules for shipping, railways and air cargo.

Coordination
Information sharing among enforcement agencies

Leveraging Technology
Control drug supply chain on internet by regulating crypto-currency markets.

Other
Stricter penalities under NDPS, effective implementation of Nasha Mukt Bharat Abhiyaan, etc.

2.6. GEOSPATIAL DATA AND NATIONAL SECURITY

Geospatial Data

- **Geospatial data** refers to any data related to any features and phenomenon related to Earth and has location as one of its attributes. It provides 3 types of information- **Location, Attribute, Temporal**
- It is captured using technologies such as **LIDAR, RADAR**, satellites and photogrammetry.

Significance of Geospatial Data in National Security

Enhancing precision and reliability of intelligence, surveillance, via GPS	Advancing situational awareness and Maritime Domain Awareness. E.g. UAVs for search and rescue operations	Supporting military operation in logistics management, developing tactical plans, etc.	Tackling new and emerging threats like cyber –attacks, hybrid warfare, etc.	Modernizing security operation e.g., Crime prediction and precision guided munitions

Steps taken by India to develop its Geospatial Capabilities

Strengthening Policy Framework National Geospatial Policy, 2022 and National Map Policy	**Institutional Development** Creation of specialised bodies like the Indian Institute of Remote Sensing.	**Educational and Research Activities** National Centre for Geodesy (NCG) has been established at IIT, Kanpur	**Advancing Satellite Capabilities** Building a network of Earth Observation Satellites (EOS) like EOS-07 NAVIC (India's own satellite-based navigation system).	**Developing Spatial Data Infrastructure** Platforms like Bharatmaps and Bhuvan support data sharing and access. Programs like PM Gati Shakti and SVAMITVA aid in large-scale geospatial data gathering.

Challenges in leverage Geospatial Data for National Security

Skill and Data Accessibility Gaps • Shortage of experts to interpret geospatial data. • Limited access to high-resolution data.	**Research Funding** Insufficient funding for advanced geospatial technologies and analytics and scattered research]	**Data Security Risks** Lack of secure systems to store sensitive geospatial data amid growing cyber threats. Weak locational privacy laws raise concerns over data misuse and surveillance.	**Inter-Governmental Coordination** Unclear rules on data sharing across central, state and local levels.

Way forward to effectively leverage Geospatial Data for National Security

Foster Collaboration Build synergy between government, academia, and industry to boost innovation and efficiency.	**Promote Specialized Education** Encourage study in fields like Geo-Informatics, big data analytics and remote sensing to build skilled professionals.	**Improve Inter-Agency Coordination** Enhance collaboration among police, defence and intelligence agencies for better data use in national security.

2.7. EMERGING DIMENSIONS OF WARFARE

2.7.1. HYBRID WARFARE

Hybrid Warfare

Hybrid Warfare is a strategy that combines conventional tactics (kinetic warfare) with unconventional methods (non-kinetic warfare), to achieve political or strategic goals without resorting to full-scale war.

Key characteristics of Hybrid Warfare

Blurred War-Peace Line	Ambiguity and Attribution	Multi-Domain Attacks	Use of Non-State Actors	Psychological Warfare (Info War)
Hard to tell when war begins, making traditional responses ineffective.	Attacks are vague and hard to trace, delaying response and accountability.	Involves land, air, sea, cyber, and space—making defence more complex.	Employs proxies and non-state groups to carry out operations.	Example: China renaming areas in Arunachal Pradesh to assert territorial claims.

Reasons for rise in Hybrid Warfare

Threat Assessment	Low-Cost	Ease of Attack	Lack of Global Rules
Hybrid threats are often missed by conventional security frameworks.	Cheaper than full-scale war and avoids direct blame. E.g., U.S. sanctions on Iran.	Cyber, AI, and digital tools make attacks easier. E.g., Russian cyberattacks on Ukraine.	No clear international laws to regulate grey-zone tactics, especially cyber warfare.

Factors making India vulnerable to Hybrid Warfare

Hostile Neighbours	Internal Unrest	Evolving Terror Tactics	Digitalisation of Economy
Pakistan and China supports terrorism, fake currency, etc.	Presence of Left-Wing Extremism and ethnic tensions in the Northeast.	Rise of lone wolf attacks and sleeper cells—hard to detect and prevent.	Threat of Cyber-attack on critical infrastructure (e.g. Possibility of Chinese malware attack on Mumbai power grid in 2021).

India's Hybrid Warfare Preparedness

Defence Modernisation	Structural Reforms	Global Partnerships	Parliamentary Oversight
Indigenous weapons like DRDO's DURGA-II Boost through 'Make in India' in defence sector	Set up CDS (Chief of Defence Staff) Created Defence AI Council and Defence AI Project Agency for tech-led planning	GSOMIA with the U.S. Quad cooperation on cyber security and defence	2024 Defence Committee reviewing cyber defence, anti-drone tech and system integration

Way ahead to combat Hybrid Warfare

Institutional Strengthening
- Regular audits of critical systems (e.g. fintech networks)
- Create a Hybrid Warfare Division for offensive and defensive action
- Whole-of-Government Strategy led by the National Security Council Secretariat

Real-Time and Tech-Based Response
- Train forces in robots, drones and smart tech
- Use real-time situational awareness tools for quicker threat detection

Global Collaboration
- Promote international cooperation with clear rules and coordinated action for grey-zone threats

2.7.2. GREY-ZONE WARFARE TACTICS

The actions undertaken by the United States against Venezuela reflect a grey-zone warfare approach.

About Grey-zone Warfare

- Grey-zone Warfare involves a set of activities that occur **between peace (or cooperation) and war (or armed conflict).**
  - It aims to harm an adversary **without** them **feeling threatened** or realising they are under attack
- **Tactics Used:** Cyber operations (Using Malwares to disrupt **Power grids, telecommunications networks,** etc.**),** Raids, special operations, proxy violence or **Salami slicing** (China's tactics) that deals with small military actions to conquer the opposition's territory piece by piece, etc.
- **Key Features**
  - **Operations below the threshold of war**: The aggressor relies on non-kinetic or indirect instruments that fall short of provoking a conventional military response.
  - **Incremental and prolonged escalation**: Actions unfold gradually sometimes over years or even decades limiting the defender's ability.
  - **Exploitation of target vulnerabilities**: Operations are tailored to political, economic, technological, or societal weaknesses of the target state.
  - **Plausible deniability and weak accountability**: The aggressor avoids acknowledging involvement.

India faces persistent grey-zone warfare from China and Pakistan. It can deal with it by **Integrating of Cyber Defence** into Military planning, Regular **red-teaming** (method of testing cybersecurity effectiveness) **of critical infrastructure**, etc.

2.7.3. BIOSECURITY AND BIOLOGICAL WEAPONS CONVENTION

Why in the News?

India hosted an international conference in New Delhi marking **50 years of the Biological Weapons Convention (BWC),** focusing on **"Strengthening Biosecurity for the Global South".**

About Biological Weapon Convention (BWC)

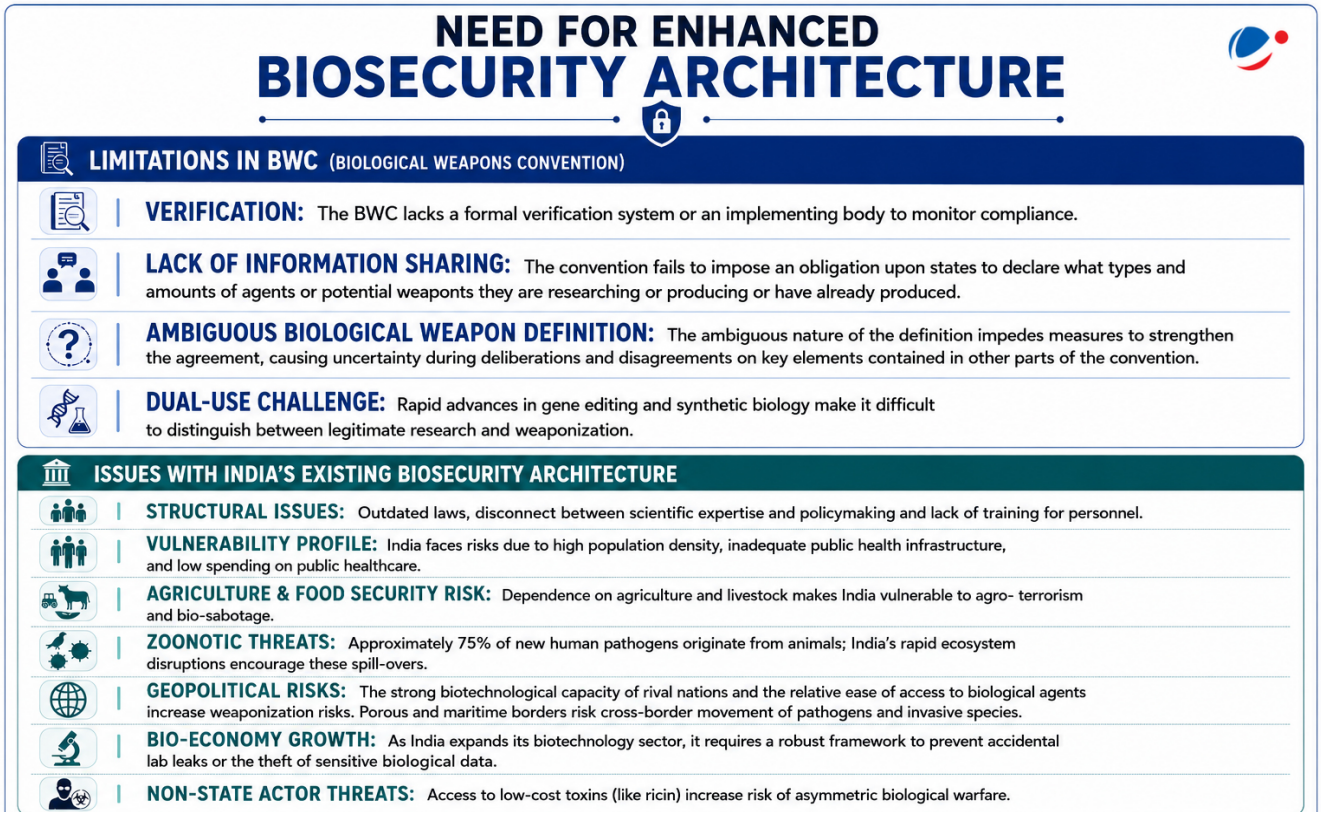
- Formally known as '**The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction'.**
- **Nature:** It was the first multilateral disarmament treaty to ban an **entire class of weapons of mass destruction (WMDs)**.
  - BWC **supplements the 1925 Geneva Protocol**, which had prohibited only the use of biological weapons.
- **Establishment:** Opened for signature on 10 April 1972 and entered into force on 26 March **1975.**
- **Membership**: 189 States Parties and four Signatory States, **India signed and ratified** in 1974.
- **Prohibitions:** The treaty bans the **development, production, acquisition, stockpiling and transfer** of biological weapons and their delivery systems.
- **Achievements of the BWC:**
  - **First Treaty:** To ban an entire class of Weapons of Mass Destruction (**WMDs).**
  - **Dismantling of bioweapons programs**: Contributed to the termination of **over 20 offensive biological weapons programs**.
  - **Reinforcement of Science Diplomacy:** Encourages integration of **scientific expertise into disarmament decision-making** and supports norms such as **voluntary codes of conduct** for scientists.

About Biosecurity

- **Definition:** Biosecurity refers to the set of practices and systems designed to **deter the intentional misuse of biological agents, toxins or technologies.**
- **Scope:** It encompasses food safety, zoonoses, management of invasive alien species and the introduction of **Living Modified Organisms (LMOs)**.
- **Specific Biosecurity Hazards**
  - **Zoonotic diseases (Zoonoses):** E.g., Avian influenza (H5N1), BSE (from cattle) and **Nipah virus** (from pigs).
  - **Agricultural Risks:** Foreign invasive species, **agriterrorism**, and the intentional release of insect vectors.
  - **Synthetic Threats:** Infectious agents built using freely available genomic knowledge on the internet and readily available building blocks.
- **India's Existing Biosecurity Architecture**
  - **Major laws:** The **Epidemic Diseases Act (1897); Disaster Management Act (2005), Environment (Protection) Act, 1986;** Livestock Importation Act, Plant Quarantine Regulatory Act; **Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005**.
  - **Regulatory bodies**:
    - **Research governance and safety frameworks**: Department of Biotechnology under Ministry of Science and Technology.
    - **Outbreak surveillance and response**: National Centre for Disease Control under Ministry of Health and Family Welfare.
    - **Livestock biosecurity and transboundary diseases**: Department of Animal Husbandry and Dairying under Ministry of Fisheries, Animal Husbandry & Dairying.
    - **Agricultural imports and exports**: Plant Quarantine Organisation of India under Ministry of Agriculture and Farmers Welfare.

Way Forward

- **New Legislation:** Draft a comprehensive **Public Health and Biosecurity Bill** to replace outdated laws, provide clear power structures and address modern threats.
- **Need for a Dedicated Biosecurity Agency in India:** It would eliminate siloing, ensuring **strategic alignment** across health, agriculture, and defense sectors.
- **One Health Integration:** Adopt a **"One Health" approach** within intelligence networks to assess risks across human, animal and plant health simultaneously.
- **Research and Development:** Focus on defence-oriented virology, vaccines and bio-threat mitigation.
- **AI Safeguards:** Formulate a nationwide task force to study biosecurity threats stemming from **AI-Bio convergence** and conduct technology foresight studies.
- **Diplomatic Leadership:** Leverage platforms like **Quad** and the **US-India iCET** for joint strategic initiatives in biosecurity detection and deterrence.


NEED FOR ENHANCED
BIOSECURITY ARCHITECTURE
LIMITATIONS IN BWC (BIOLOGICAL WEAPONS CONVENTION)
VERIFICATION: The BWC lacks a formal verification system or an implementing body to monitor compliance.
LACK OF INFORMATION SHARING: The convention fails to impose an obligation upon states to declare what types and amounts of agents or potential weaponts they are researching or producing or have already produced.
AMBIGUOUS BIOLOGICAL WEAPON DEFINITION: The ambiguous nature of the definition impedes measures to strengthen the agreement, causing uncertainty during deliberations and disagreements on key elements contained in other parts of the convention.
DUAL-USE CHALLENGE: Rapid advances in gene editing and synthetic biology make it difficult to distinguish between legitimate research and weaponization.
ISSUES WITH INDIA'S EXISTING BIOSECURITY ARCHITECTURE
STRUCTURAL ISSUES: Outdated laws, disconnect between scientific expertise and policymaking and lack of training for personnel.
VULNERABILITY PROFILE: India faces risks due to high population density, inadequate public health infrastructure, and low spending on public healthcare.
AGRICULTURE & FOOD SECURITY RISK: Dependence on agriculture and livestock makes India vulnerable to agro- terrorism and bio-sabotage.
ZOONOTIC THREATS: Approximately 75% of new human pathogens originate from animals; India's rapid ecosystem disruptions encourage these spill-overs.
GEOPOLITICAL RISKS: The strong biotechnological capacity of rival nations and the relative ease of access to biological agents increase weaponization risks. Porous and maritime borders risk cross-border movement of pathogens and invasive species.
BIO-ECONOMY GROWTH: As India expands its biotechnology sector, it requires a robust framework to prevent accidental lab leaks or the theft of sensitive biological data.
NON-STATE ACTOR THREATS: Access to low-cost toxins (like ricin) increase risk of asymmetric biological warfare.

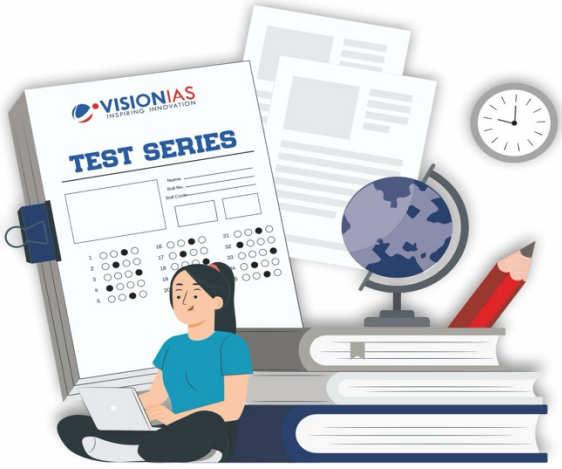
Conclusion

Biosecurity has evolved from a narrow focus on biological weapons to a **holistic "One Biosecurity" concept** integrating human, animal, and environmental health. For India, transforming regulatory deficits into diplomatic strength offers an opportunity to lead the **Global South** in championing modern, resilient biosecurity norms.

ALL INDIA PRELIMS TEST SERIES

Get the Benefit of Innovative Assessment System from the leader in the Test Series Program

- General Studies (हिन्दी माध्यम में भी उपलब्ध)
- CSAT (हिन्दी माध्यम में भी उपलब्ध)
  - VISION IAS Post Test Analysis™
  - Flexible Timings
  - ONLINE Student Account to write tests and Performance Analysis
  - All India Ranking
  - Expert support - Email / Telephonic Interaction
  - Monthly Current Affairs



2027 | ENGLISH MEDIUM 28 JUNE | हिन्दी माध्यम 28 जून

Scan QR code for instant personalized mentoring

2.7.4. SPACE WEAPONISATION

Space Weaponisation

- **Space Weaponisation** includes placing weapons in outer space as well as creating weapons that will destroy targets in space.
- It is different from the **militarization of space** that assists armies on the conventional battlefield.

Implications of space weaponisation

Fear of war
Increases chances of conflict, just like the US–USSR space race during the Cold War.

Threat to Peaceful Space Use
Hampers scientific and commercial missions like the Hubble Telescope and space research.

Space Debris Hazard
Over 40,500 debris objects (larger than 10 cm) now orbit Earth, risking collisions (European Space Agency).

Risk to Critical Infrastructure
Weaponised space could target Earth-based systems like India's IRNSS navigation satellites.

Reasons behind space weaponisation

Gaining War Superiority
Space control enhances dominance across land, sea, air and cyber warfare.

Protecting Satellites
Countries develop ASAT (Anti-Satellite) weapons to defend their space assets.
Example: India's Mission Shakti

Dual-Use Technology
Many space tools like GPS have both military and civilian uses, making them strategic.

Weak Space Treaties
Agreements like the Outer Space Treaty (OST) lack strict enforcement, leaving loopholes for weaponisation.

Key initiatives to prevent space weaponisation

Outer Space Treaty (1967)
Promotes peaceful use of outer space.
Prohibits placement of nuclear weapons or weapons of mass destruction in space.

PAROS (Prevention of an Arms Race in Outer Space)
UN initiative calling for a ban on space weapons (still under negotiation)

Partial Test Ban Treaty (1963)
Bans nuclear tests in space, underwater and the atmosphere.
Aimed at limiting space militarisation.

Artemis Accords
Framework for peaceful lunar exploration and cooperation.

Way forward to prevent space weaponisation

Space as a Global Commons
Treat outer space like international waters—used peacefully by all.

Legally-Binding Treaty
Enforce PAROS and make it legally binding

Space Domain Awareness
Boost monitoring systems (e.g., Combined Space Operations Initiative) to detect threats and manage debris.

Transparency and Trust Building
Countries must share accurate data with the UN Office for Outer Space Affairs (UNOOSA) to build trust and reduce misunderstandings.

2.8. KEYWORDS

Keywords			
Hybrid Warfare	Grey-Zone Warfare	Salami Slicing	Information Warfare
Psychological Warfare	Proxy Warfare	Non-State Actors	Multi-Domain Warfare
Cyber Warfare	AI Warfare	Autonomous Systems	Directed Energy Weapons
Biosecurity	One Health	Biological Weapons Convention	Bio-Terrorism
Space Weaponisation	Mission Shakti	PAROS	Outer Space Treaty
Space Debris	Space Domain Awareness	DURGA-II	Strategic Deterrence
Plausible Deniability	Influence Operations	Narrative Warfare	Cognitive Warfare

2.9. PRACTICE QUESTION

Hybrid warfare has blurred the distinction between war and peace. Discuss its implications for India's national security.

Introduction	Body Part: 1	Body Part: 2	Conclusion
Define hybrid warfare.	Characteristics and instruments.	Implications for India.	Need for integrated security responses.

VISIONIAS
DAKSHA MAINS
MENTORING PROGRAM 2026
DAKSHA MAINS MENTORING PROGRAM 2026
(A Strategic Revision, Practice, and Enrichment Mentoring Program for Mains Examination 2026)
DATE
6 July
DURATION
5 Months
HIGHLIGHTS OF THE PROGRAMME
Highly experienced and qualified team of mentors
Emphasis on score maximization and performance improvement
Scheduled group sessions for strategy discussions, live practice, and peer interaction
Personalized one-to-one sessions with mentors
Well-structured revision and practice plan for GS Mains, Essay & Ethics
Subject-wise strategy documents based on thorough research
Access toDaksha Mains Practice Tests
Continuous performance assessment, monitoring and smart interventions
For any assistance call us at:
+91 8468022022, +91 9019066066
enquiry@visionias.in

3. SECURITY CHALLENGES AND THEIR MANAGEMENT IN BORDER AREAS

3.1. SECURITY ISSUES IN BORDER AREAS

3.1.1. INDIA AND BORDERING COUNTRIES

India and Bordering Countries

Border | Challenges along Border | Initiatives taken

Border	Challenges along Border	Initiatives taken
India-China	• Border disputes at **Galwan Valley, Aksai Chin, Arunachal Pradesh, Doklam** etc. • Inadequate infrastructure (access to rail, road etc.) due to high altitude terrain. • Water- sharing issues (e.g. **Brahmaputra River**).	• Creating infrastructure to reduce time for troop movement like **Dhola- Sadiya Bridge**. • Development of North East Region. E.g. Border Area Development Programme, Vibrant Village programme for border village development. • Army infrastructure projects within 100 km of LAC exempted from forest clearance.
India-Pakistan	• Border dispute at **Sir Creek** and **Kashmir**. • Infiltration and Cross-border terrorism. E.g. **Uri ,Pulwama** and **Pahalgam** • Drones used for smuggling arms and narcotics across the border in **Punjab** • Diverse terrain including desert, marshes, snowcapped mountain and plains. • Time & cost overruns in infrastructure projects	• Comprehensive Integrated Border Management System (**CIBMS**) To improve situational awareness at different levels of hierarchy. • **BIM** (Border Infrastructure and Management) Scheme: for developing infrastructure along India's international borders. • Decision for deploying **National Security Guard** commandos in **J&K** to counter terror operations by training J&K police and other paramilitary forces. • Suspension of **Indus water treaty (1960)**.
India-Nepal	• Border dispute at **Kalapani, Limpiyadhura** and **Lipulekh**. • Fear of spread of **Maoist** insurgency due to links of **Nepal's Maoists** in India. • Easy escape & illegal activities like drugs and arms smuggling, etc. • **Chinese** investment in core sector of Nepal like infrastructure, hydro energy, etc.	• Establishment of Border District Coordination Committee. • Construction of over **1300 km** of roads along border. • Development aid to Nepal. (In FY 2026-27, India allocated **Rs. 800 crore** in aid to Nepal) • Security related infrastructure development like **Fatehpur Border out Post**.
India-Bhutan	• Insurgency. E.g. United Liberation Front of Asom (**ULFA**) camps in Bhutan. • Smuggling of goods like Bhutanese cannabis. • Open Cross-Border Movement led to human trafficking and smuggling of migrants.	• **Operation All Clear** by Royal Bhutan Army to remove insurgents camps in Bhutanese territory. • Establishing new border posts in **Sikkim**. • General approval under **Forest (Conservation) Act, 1980** for diversion of forest land for infrastructure projects.
India-Myanmar	• Drug trafficking due to proximity to death/golden triangle. • border is porous, poorly guarded, and lies in a remote, insurgency-prone area. •	• Integrated Check Posts to strengthen ties with **SAARC, Thailand** and **Myanmar**. • **Operation Sunrise** targeting insurgents along the India-Myanmar border. • Proposal of fencing entire **1643-kilometer-long** Indo-Myanmar border.
India-Bangladesh	• Illegal migration into India (around **20 million** as per **2016**). • Smuggling of goods like **jamdani** sarees.	• India-Bangladesh Land Boundary Agreement, **2015**. • Establishment of Border Protection Grid (**BPG**). • **BOLD-QIT** was implemented under the **CIBMS** scheme.

3.2. SUDARSHAN CHAKRA MISSION

Why in the News?

Prime Minister announced the launch of **Mission Sudarshan Chakra** during the 79th Independence Day celebrations.

More on the news

- The mission seeks to develop **Air Defence system aimed at neutralising enemy defence infiltrations and enhancing India's offensive capabilities.**
- **Additionally,** The Indian Air Force is pressing for rapid progress on **Project Kusha**, an indigenous initiative led by **DRDO** to develop **a long-range air defence missile system.**

Project Kusha
- **Developing Body: DRDO** and **Bharat Electronics Limited.**
- **Aim:** An indigenous initiative to develop **a long-range air defense missile system.**
  - Seeks to develop **Long-Range Surface-to-Air Missiles or LR-SAM.**
- **Expected by:** 2028–2029.

About Sudarshan Chakra Mission

- **Objectives:**
  - To strengthen India's deterrent and offensive capabilities by expanding, strengthening and modernising **national security shield.**
  - It will be part of **Multi-Layered Missile Defence System** of India.
- **Features:**
  - **Timeline:** Mission to be completed by **2035**.
  - **Comprehensive Protection:** It will **safeguard India's strategic, civilian and religious sites/assets** (e.g. hospitals, railways).
  - It will cover all public places with an expanded nationwide security shield across air, land and sea.
    - The mission will be integrating advanced surveillance, cyber protection and physical infrastructure safeguards.
    - It will be a system for **targeted precise action**.
  - **Indigenous technology:** It will be entirely researched, developed and manufactured in India.
  - **Air Superiority:** Provides protective cover for ground troops**.**
  - **Deterrence Effect:** Creates a strong deterrent against potential enemy aggression**.**
  - **Self-Reliance:** The mission will promote self-reliance in defence modernisation**.**

Conclusion

The Sudarshan Chakra Mission epitomizes the blend of India's cultural legacy and modern technological excellence, reinforcing the nation's resolve to proactively safeguard its sovereignty.

Related News: DRDO successfully conducts maiden flight-tests of Integrated Air Defence Weapon System (IADWS)

IADWS is expected to offer multiple layers of protection by **combining surveillance, threat identification and air defence systems**.

About IADWS

- **Key Components: Indigenous Quick Reaction Surface to Air Missiles (QRSAM):** Developed by DRDO.
  - It is a short-range (5 to 30 km range) SAM system designed to protect moving armoured columns from aerial attacks. It is configured on mobile platform and is capable of providing air defence on the move.
  - **Advanced Very Short Range Air Defence System (VSHORADS) missiles:** Developed by Research Centre Imarat (RCI).
    - It is a **Man Portable Air Defence System (MANPADS)** designed to neutralize low-altitude aerial threats at short ranges.
  - **A high-power laser-based Directed Energy Weapon (DEW):** Developed by Centre for High Energy Systems and Sciences.

> **Laser-DEW** can **engage targets at the speed of light** and use an intense laser beam to cut through the target.

- **Command Centre:** Integrated operation of all the weapon system components is controlled by a **Centralised Command and Control Centre** developed by Defence Research & Development Laboratory (DRDL).

3.3. QUANTUM TECHNOLOGIES IN ARMED FORCES

Why in the News?

Chief of Defence Staff released the **Military Quantum Mission Policy Framework**, a comprehensive document that includes the policy and the road map to implement Quantum Technologies in the Armed Forces.

Key Highlights of the Framework

- **Vision:** It aims for jointness and integration among the Tri-Services to achieve technological dominance in future battlefields and prepare for technology-centric warfare.
- **Civil-Military Fusion:** Aligned with National Quantum Mission (NQM) to ensure collaboration between civilian research and military applications through dedicated governing bodies.
  - **NQM** aims **to build a strong national ecosystem** spanning R&D, infrastructure, startups, and skilled human resources with a budget outlay of ~6,000 crores (2023-24 to 2030-31).
- **Core Domains:** Prioritises four critical quantum pillars:
  - Quantum Communication
  - Quantum Computing
  - Quantum Sensing & Metrology
  - Quantum Materials and Devices

APPLICATIONS OF QUANTUM TECHNOLOGY IN MILITARY

APPLICATION AREA	QUANTUM TECHNOLOGY CAPABILITY	ADVANTAGE OVER EXISTING TECHNOLOGY
NAVIGATION & POSITIONING	Atomic interferometry enables highly precise navigation for missiles and submarines.	Reduces dependence on satellite-based navigation (GPS), which is vulnerable to jamming, spoofing and anti-satellite weapons.
SENSING & METROLOGY	Quantum magnetometers (e.g., SQUIDs) and gravimeters detect minute magnetic or gravitational anomalies.	Enhanced sensitivity to detect submerged submarines and hidden underground structures beyond the reach of classical sensors.
WARFARE CAPABILITIES	Quantum-enabled AI powers autonomous drones and robotic systems.	Faster and more efficient processing of complex battlefield variables.
QUANTUM IMAGING	Entangled-photon and ghost-imaging techniques enable imaging through fog, smoke, or darkness.	Outperforms optical/thermal cameras that struggle in low-light or obscured environments.
SECURE COMMUNICATION	Quantum Key Distribution (QKD) and entanglement generate theoretically unhackable keys.	Stronger than classical encryption, which can be intercepted or broken by advanced computational power without detection.
QUANTUM MATERIALS	Develops aerospace materials with adaptive properties, such as changing camouflage.	Offers dynamic, molecular-level adaptability and superior resilience compared to standard composite materials.
CHIP INSPECTION	Quantum sensors read magnetic "fingerprints" to detect manufacturing defects or hardware "Trojans".	Enables highly precise, non-destructive screening of microchips; better than destructive traditional deep-inspection methods.
LOGISTICS OPTIMIZATION	Quantum algorithms solve complex optimization problems like routing supply chains.	Handles massive datasets and interconnected variables exponentially faster than classical computers in complex scenarios.

Conclusion

India's quantum security strategy must integrate technology monitoring, research flexibility, and supply chain security while leveraging global partnerships and domestic innovation. A proactive, multi-pronged approach will ensure national security remains resilient in the quantum era.

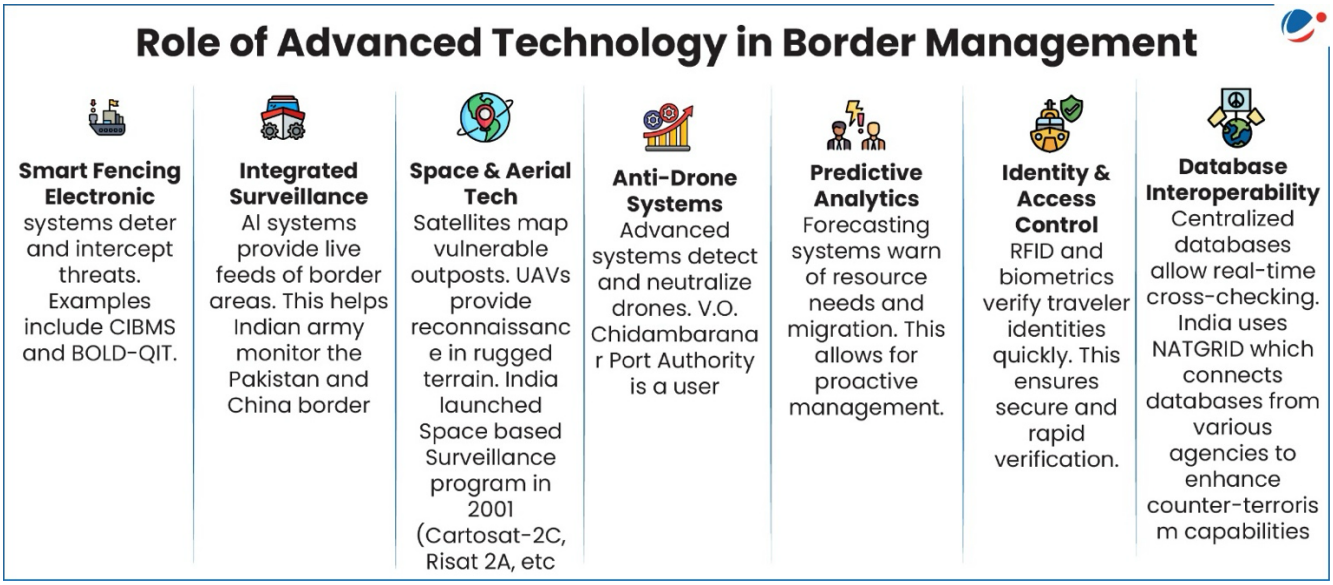
3.4. ADVANCE TECHNOLOGY & BORDER MANAGEMENT

Why in the News?

Recently, the Union Home Minister emphasised the need to adopt advanced technological solutions to effectively address the new challenges posed by adversaries along borders.

Need for Advanced Technology in Border Management

- **Countering New Infiltration Tactics (Drones and Tunnels)**:
  - E.g., a surge in **drone** incursions dropping **narcotics and weapons**, particularly in the western sector.
  - Organized criminal networks are highly adaptable, frequently using encrypted communications and advanced surveillance to elude detection.
- **Terrain:** Managing **unfenced gaps** in difficult terrain like the **shifting eastern riverine borders** and marshes of Gujarat.
- **Cyber & Electronic Warfare**: E.g., attacks on border surveillance infrastructure and communication networks.
- **Relieving Troop Fatigue and Centralizing Command**: Traditional border guarding is incredibly manpower-intensive, which tires out troops and reduces operational efficiency.
- **Protecting the Maritime and Underwater Domain**: Border security is expanding beyond land and airspace into the maritime and subsea environments. E.g. 26/11 attacks


Role of Advanced Technology in Border Management
Smart Fencing Electronic systems deter and intercept threats. Examples include CIBMS and BOLD-QIT.
Integrated Surveillance AI systems provide live feeds of border areas. This helps Indian army monitor the Pakistan and China border
Space & Aerial Tech Satellites map vulnerable outposts. UAVs provide reconnaissance in rugged terrain. India launched Space based Surveillance program in 2001 (Cartosat-2C, Risat 2A, etc
Anti-Drone Systems Advanced systems detect and neutralize drones. V.O. Chidambaranar Port Authority is a user
Predictive Analytics Forecasting systems warn of resource needs and migration. This allows for proactive management.
Identity & Access Control RFID and biometrics verify traveler identities quickly. This ensures secure and rapid verification.
Database Interoperability Centralized databases allow real-time cross-checking. India uses NATGRID which connects databases from various agencies to enhance counter-terrorism capabilities

Measures to promote Integration of Technology in Border Management

- **Expanding Existing Surveillance Infrastructure**
  - **Wider Rollout of CIBMS:** Following pilot projects like BOLD-QIT, the Stage II and Stage III of the CIBMS shall be implemented, which will cover approximately 1,955 kilometers of vulnerable borders.
  - **AI-Powered Monitoring:** E.g., The Border Security Force (BSF) is planning to introduce a unified "smart border observation and monitoring system".
  - **Other**: Invest in solar-powered surveillance towers, satellite-based communication and automated drone monitoring to overcome the severe lack of digital infrastructure, reliable power and high-speed internet in remote border regions.

- **Operational Enhancements: E.g.,** Establish a unified digital command and control system to overcome inter-agency fragmentation.
  - This system should integrate all border security agencies into a centralized network.
- **Create a Border Security Technology Oversight Authority:** It shall be tasked with reviewing and auditing surveillance operations to ensure they comply with legal frameworks and prevent misuse.

Conclusion

Effective border management in India increasingly requires the integration of **advanced technologies such as smart fencing, AI-based surveillance, and anti-drone systems**. Learning from global systems like Israel's Smart Fence, US's Integrated Fixed Towers, we need to strengthen our indigenous innovation, infrastructure, and inter-agency coordination which will be crucial to tackle emerging threats and safeguard India's territorial integrity.

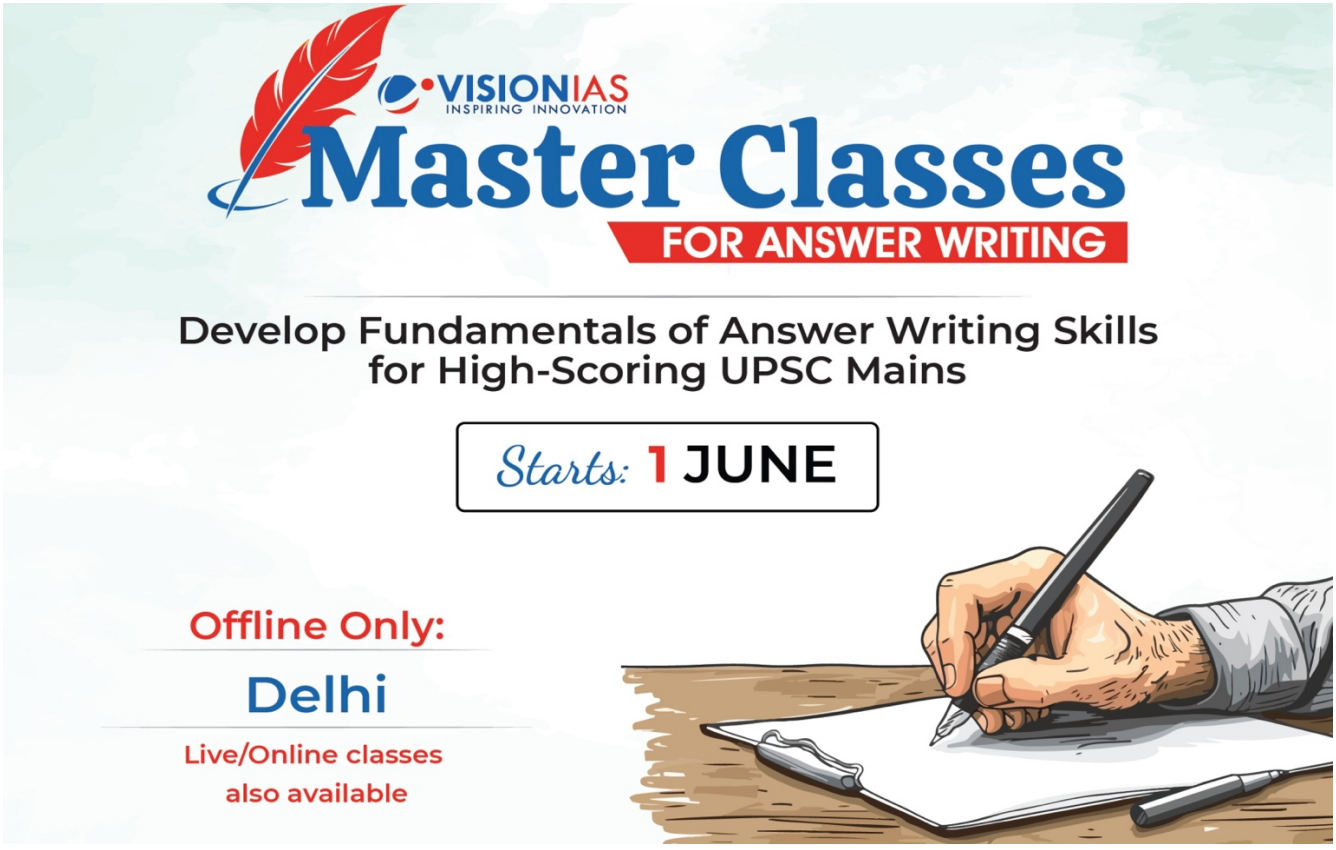
3.5. KEYWORDS

Sudarshan Chakra	BOLD QIT	Anti Drone System	MANPADS
Smart Fencing	Atomic Interferometry	National Quantum Mission	Project Kusha

PRACTISE QUESTION

Discuss the role of advanced technology in border management.

Introduction	Body Part 1	Conclusion
Start with recent examples.	Discuss the role of advanced technologies like smart fencing, RFID, etc.	Conclude with some steps that India has taken.



4. MARITIME SECURITY AT A GLANCE

Maritime Security

Maritime Security involves protecting the nation's sovereignty from threats arising from the oceans and seas.

India's Maritime Security Architecture

Indian Navy (IN)	Indian Coast Guard (ICG)	Border Security Force (BSF)	Central Industrial Security Force (CISF)	Sagar Suraksha Dal:
Responsible for overall maritime security.	Responsible for coastal security in the territorial waters, including areas to be patrolled by the marine police.	Responsible for the security and surveillance of the creeks in Gujarat and the Sunderbans.	Responsible for the physical security of India's major ports	Fishermen groups, composed of trained volunteers, monitor the seas and coastal waters

Need of Maritime Security for India

Vulnerabilities of coastline	Geostrategic interests	Economic development
Maritime terrorism like 26/11 Mumbai attack, Piracy, Smuggling, Infiltration through creeks.	Like countering Chinese influence, becoming a net security provider and executing HADR operations in IOR.	Around **80%** of India's external trade and **90%** of energy trade happens through IOR.

Challenges to Maritime Security

Piracy and Maritime Terrorism in IOR	Maritime Border Disputes with neighbouring countries, such as Pakistan, Sri Lanka	Rising Influence of USA and China like Chinese dual-use facilities in Myanmar and Sri Lanka	Lackadaisical State Government: Issues include underused patrol boats, delayed infrastructure, manpower shortages, and unspent funds (CAG Report).	Environmental Challenges: Climate change (rising seas, extreme weather), natural disasters (tsunamis, cyclones) Marine pollution (Oil spills)
E.g. Indian Navy rescued the hijacked Bulgarian vessel 'Ruen' in 2024.				

Steps taken by India to strengthen Maritime Security

Coastal Surveillance & Coordination	Maritime Theatre Command (MTC)	Information Sharing	Regional Maritime Cooperation	Coastal Shipping Act, 2025
Sagar Kavach coastal security exercises to test and enhance preparedness of all maritime security agencies	Proposed to create efficient deployment of maritime assets across the Navy, Army and Air Force.	IFC-IOR (Information Fusion Centre – Indian Ocean Region) of Indian Navy to enable real-time maritime domain awareness.	Initiatives like SAGAR, MAHASAGAR, IORA, and IONS (Indian Ocean Naval Symposium) to boost diplomatic and naval collaboration in the Indian Ocean Region.	Seeks to regulate vessels engaged in trade within Indian coastal waters.

Way Forward to strengthen maritime security

5-point framework	Strengthening the surveillance system	Unified Command Structure	Operationalize Blue Economy Potential	Boost Maritime Diplomacy
Free trade, dispute resolution, connectivity, threat response, environmental protection	Through advanced coastal radar networks. E.g. High Frequency Radar	Expedite the formation of a unified Maritime Theatre Command to ensure integrated operations.	Secure India's interests in deep-sea mining, offshore energy and sustainable fisheries.	Deepen cooperation through IORA, IONS, QUAD, and SAGAR and conduct joint naval exercises to increase interoperability and trust

AHMEDABAD | BENGALURU | BHOPAL | CHANDIGARH | DELHI | GUWAHATI | HYDERABAD | JAIPUR | JODHPUR | LUCKNOW | PRAYAGRAJ | PUNE | RANCHI ©Vision IAS

4.1. DEFENCE MODERNISATION

Modernisation of Armed Force

Modernisation involves continuously upgrading weapons, platforms, and technologies to keep the armed forces ready for evolving security threats and strengthen overall defence capabilities.

Need for Modernisation of Armed Forces

Challenging strategic environment like **assertiveness of China** in Indian Ocean.	**Inadequate number of equipments** like aircraft, submarines etc.	Rapidly changing landscape of warfare like **hybrid warfare, cyberwarfare**, etc.	Enhancing **HADR capabilities** in which defence forces play the critical role.

Challenges in modernisation of Armed Forces

Budget Allocation Issues A large portion of the defence budget goes to salaries, pensions, Leaving limited funds for capital expenditure and **R&D** for new technology	**Slow Decision-Making.** It can take **7–9 years** to finalise production and acquisition contracts.	**Technological Limitations** India lacks the **deep ecosystem** to indigenously design and manufacture advanced defence systems and critical components.	**Stalled Structural Reforms** Important reforms like **Integrated Theatre Commands** are delayed due to inter-service rivalries and lack of consensus among the three forces.

Steps taken by India for mordernisation of Armed Forces

Defence Reforms 2025 declared as the **Year of Reforms**, Inter-Services Organisations Act, 2023 and empowering **Chief of Defence Staff (CDS)** to issue joint orders across all three forces to boosts coordination among 3 forces.	**Indigenisation and Innovation** Defence Acquisition Procedure **(DAP) 2020**, Positive Indigenisation List, and **SRIJAN Portal**, Schemes like **ADITI** and **iDEX** promote startups and **MSMEs** in defence.	**R&D Push** **25%** of defence R&D budget reserved to promote indigenous defence technology, **74% FDI** allowed via automatic route and **100%** via government approval to boost investment.	**Space Warfare Preparedness** **Mission DefSpace** supports innovation in space-based defence applicartions, **Mission Shakti (ASAT)** to defend India's space assets from threats.

Way forward for mordernisation of Armed Forces

Ensure Steady Funding: Create a Non-Lapsable Defence Modernisation Fund (as proposed by the **15th Finance Commission**).	**Implement Reforms** Set up **BRADS** (Board of Research for Advanced Defence Sciences) as recommended by the **Rama Rao Committee.**; **Shekatkar Committee** recommendations to boost combat capability and rebalance defence spending	**Boost Private Sector Role** Support industry using the **5Is** (Identify, Incubate, Innovate, Integrate, and Indigenous. Partnerships), implementation strategy for **AMCA** project is a positive step in this direction.
Strengthen Collaboration Build strong industry-defence-academia partnership	**Comprehensive Defence Modernisation Roadmap** Focuses on advanced weapons systems, cyber and electronic warfare, jointness in armed forces, etc.	

4.2. THEATERISATION OF DEFENCE

Why in the news?

Recently, Air Chief Marshal cautioned against rushing the theaterisation plan.

What is theaterisation of defence?

- **Aim:** To bring together the Army, Navy and Air Force under specific 'theatre' commands.
  - All resources will be placed **under one unified command structure** for better coordination and deployment.
- **Theatre Commands:** Each command will be assigned a specific geographical region, combining the resources of the three services for operational roles.
  - This unified command replaces the current **17 separate service-specific commands (7 Army, 7 Air Force, 3 Navy)** that now work independently.

NEED FOR
THEATERISATION
ADDRESSING COORDINATION GAPS
E.g., during the Kargil War, along with other reasons, poor coordination delayed the employment of air power.
MODERN WARFARE NEEDS
Coordination is required not only among land, sea, and air forces but also across new domains like UAVs, precision weapons, cyber, and space.
STRATEGIC THRUST AND DETERRENCE
China's PLA operates an integrated Western Theatre Command along the border of India.
Engaging with it with multiple separate commands makes our approach complex.
ONE THEATRE ONE COMMAND
Integrated • Agile • Decisive
ENGAGING WITH IT WITH MULTIPLE SEPARATE COMMANDS MAKES OUR APPROACH COMPLEX
Engaging with it with multiple separate commands makes our approach complex.
RESOURCE EFFICIENCY
Theaterisation rationalises military structures by eliminating duplication across the 17 existing commands (each with its own headquarters, logistics, and training).
SWIFT DECISION-MAKING
SENSOR
THEATRE COMMANDER
SHOOTER
A single theatre commander ensures unity of effort and the authority that can shorten the sensor-to-shooter loop, enabling decisive action.
Theaterisation enhances integration, strengthens deterrence, optimises resources, and enables faster, more decisive military action.

Steps taken towards Theaterisation

- **Chief of Defence Staff (CDS) in 2019:** Acts as the principal military adviser to the Defence Minister on tri-Service matters.
  - The CDS **strengthens unified leadership and fosters integration** for a more coordinated and modern Indian military.
- **Department of Military Affairs (DMA) in 2020:** With **CDS** as **Secretary** to facilitate optimal utilization of resources and **promote jointness** among the three Services.

- **Inter-Services Organisations (Command, Control and Discipline) Act, 2023**: For joint commanders to exercise cross-service command and discipline over personnel from any service attached to an Inter-Service Organisation (ISO).
    - **Currently, there are 3 ISOs:** Andaman and Nicobar Command, the Defence Space Agency and the National Defence Academy.
- **Joint Logistic Nodes (JLNs):** Established and operational since **2021** at **Mumbai**, **Guwahati** and **Port Blair** for **logistics integration** between the **three services**.
- **Strategic Forces Command (2003):** Responsible for handling, securing, storing and launching the country's nuclear weapons.
- **Integrated Air Command and Control System (IACCS) of the Indian Air Force:** Provides real-time coordination, enabling synchronized responses across multiple units of the three forces.
- **Headquarters Integrated Defence Staff (HQ IDS):** Established to provide an institutional framework for managing defence at a higher level and to integrate the three Services.

Challenges

- **Inter-Service Dissonance:** The Army's dominance in **budget and manpower** creates concerns about an imbalance in command influence and resource distribution.
- **Transition Difficulties:** Dismantling existing command structures is seen as a potentially **disruptive impact** on combat readiness during transition.
- **Domain Knowledge & Command:** Concerns exist regarding a **theatre commander** from one service effectively commanding and understanding the intricacies of another service's assets, particularly air power.
- **Cost and Industrial Base:** Slow growth of a robust military-industrial complex raises concerns about the cost-effectiveness and sustainability of theatreisation.

Way ahead

- **Defence Industrial Base**: India needs to increase the pace of defence indigenisation, resulting in a wider defence industrial base, helping to deal with resource challenges
- **Bridging the Divide:** Harmonize doctrines among the Army, Navy, and Air Force; update training curricula to include joint operational planning, logistics and warfighting.
- **Developing Core Strategy Documents**: The transition should be supported by clearly defined national goals and strategies achieved through multi-stakeholder consultations.
- **Adopting a cautious approach**: E.g. Structural changes to the HQ IDS and Service HQs can precede the actual raising of theatre commands to ensure support structures are in place.
- **Replication of functional Integration Model:** This model combines forces with similar functions to allow for centralized control over scarce resources, **Eg US Cyber Command**

4.3. INDIA'S JOINT DOCTRINE FOR MULTI-DOMAIN OPERATIONS

Why in the News?

Raksha Mantri released the Joint Doctrine for Multi-Domain Operations.

What is Multi-Domain Operations (MDO)?

- **Definition:** The coordinated, integrated, and synchronized employment of military forces alongside non-military national capabilities across the Land, Sea, Air, Space, Cyber and Cognitive domains.
- **Key Features:**
    - **Whole-of-Nation Approach:** A strategic framework that fuses military strength with civilian innovation, incorporating stakeholders like intelligence agencies, the private sector, and academia to achieve national objectives.
    - **Simultaneous Convergence:** The orchestration of kinetic and non-kinetic activities across all domains to present adversaries with simultaneous challenges, which severely complicates and disrupts their decision-making cycles.

Domain	Key Role
Land	Ground operations across physical terrain and human environments.
Sea	Maritime security, power projection, and protection of trade routes.
Air	Reconnaissance, strike missions, air superiority, and UAV operations.
Space	Communications, surveillance, imagery, and navigation support.
Cyber	Protection and exploitation of digital networks and critical infrastructure.
Cognitive	Influence operations targeting perception, information, and decision-making.

Differences Between MDO and Joint Operations

Aspect	Joint Operations	Multi-Domain Operations (MDO)
Space	Coordinated efforts of different military branches	Seamless integration across involved military and non-military assets/entities
Forces Involved	Army, Navy and Air Force working in collaboration	Military and non-military entities including space agencies, cyber specialists, IT firms/specialists, government agencies, and private-public defence ecosystem
Decision-Making & Collaboration	Hierarchical and structured	Decentralised and adaptive
Technology Integration	Limited to specific force capabilities	High-level integration using AI, Big Data Analytics (BDA), analytical tools, autonomous systems, and advanced sensors across domains
Operational Tempo	Sequential and phased; distinct OODA cycle	Continuous and simultaneous across domains; compressed/merged OODA cycle
Operational Picture	Whole-of-Military	Whole-of-Military and Non-Military (Whole-of-Nation)

4.4. JOINT DOCTRINE FOR CYBERSPACE OPERATIONS

Why in the News?

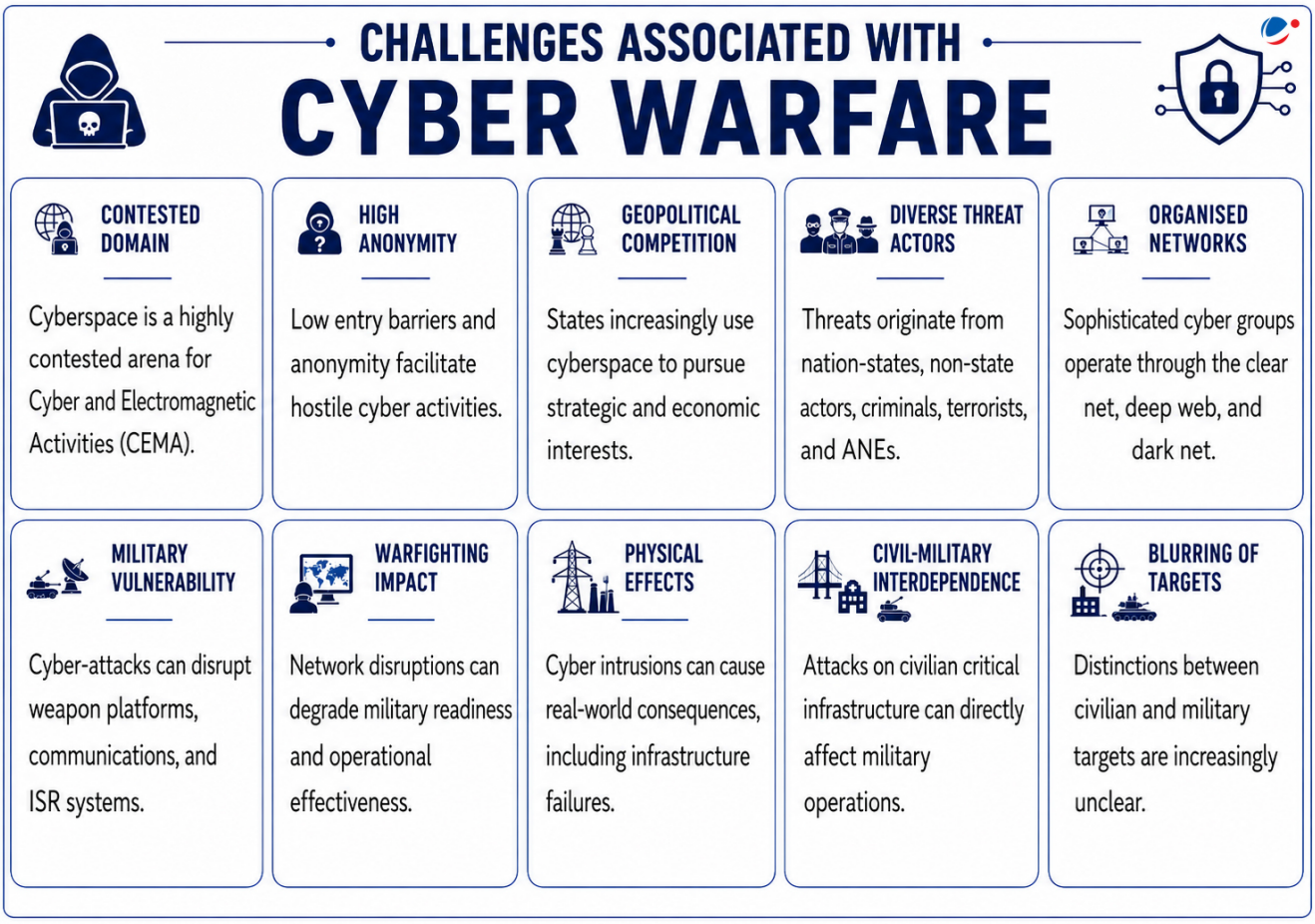
Chief of Defence Staff (CDS) and Secretary, Department of Military Affairs released the declassified versions of the Joint Doctrines for Cyberspace Operations.

Recent Examples of Cyber Warfare

- **Russia–Ukraine Conflict (2025):** Russia employed state-backed cyber operations and AI-enabled tools to target Ukrainian government, defence, and critical infrastructure.
- **India–Pakistan Conflict (Operation Sindoor, 2025):** Pakistan-sponsored actors launched millions of cyber intrusions against Indian networks, combining DDoS attacks, phishing, website defacements, and deepfake-driven disinformation.
- **Israel–Iran Conflict (2025–26):** Cyber operations complemented kinetic warfare, featuring cryptocurrency theft, intelligence gathering, psychological operations, and retaliatory DDoS and data-wiping attacks.

AHMEDABAD | BENGALURU | BHOPAL | CHANDIGARH | DELHI | GUWAHATI | HYDERABAD | JAIPUR | JODHPUR | LUCKNOW | PRAYAGRAJ | PUNE | RANCHI ©Vision IAS

- **US–Venezuela Conflict (Operation Absolute Resolve, 2026):** US cyberattacks triggered targeted blackouts and telecom disruptions, enabling follow-on air operations.
- **Thailand–Cambodia Border Dispute (2025):** Border clashes were accompanied by reciprocal cyberattacks, primarily involving DDoS campaigns and website defacements.


CHALLENGES ASSOCIATED WITH
CYBER WARFARE
CONTESTED DOMAIN
Cyberspace is a highly contested arena for Cyber and Electromagnetic Activities (CEMA).
HIGH ANONYMITY
Low entry barriers and anonymity facilitate hostile cyber activities.
GEOPOLITICAL COMPETITION
States increasingly use cyberspace to pursue strategic and economic interests.
DIVERSE THREAT ACTORS
Threats originate from nation-states, non-state actors, criminals, terrorists, and ANEs.
ORGANISED NETWORKS
Sophisticated cyber groups operate through the clear net, deep web, and dark net.
MILITARY VULNERABILITY
Cyber-attacks can disrupt weapon platforms, communications, and ISR systems.
WARFIGHTING IMPACT
Network disruptions can degrade military readiness and operational effectiveness.
PHYSICAL EFFECTS
Cyber intrusions can cause real-world consequences, including infrastructure failures.
CIVIL-MILITARY INTERDEPENDENCE
Attacks on civilian critical infrastructure can directly affect military operations.
BLURRING OF TARGETS
Distinctions between civilian and military targets are increasingly unclear.

Way Forward

- **Indigenisation and Atmanirbharta:** Develop indigenous cyber hardware, software, operating systems, and audit frameworks to reduce supply-chain risks.
- **Cyber Training:** Standardise cyber education through Centres of Excellence (CoEs), cyber ranges, and Capture the Flag (CTF) exercises.
- **Secure Supply Chain:** Strengthen Defence Critical Information Infrastructure (DCII) security through rigorous testing and certification.
- **Cyber Diplomacy:** Enhance international cooperation, norm-building, and best-practice exchanges.
- **Emerging Technologies:** Harness Quantum Technologies, Advanced Cryptography, User Behavioural Analytics (UBA), and micro-segmentation.
- **Zero Trust Architecture (ZTA):** Implement continuous identity and access verification across defence networks.
- **Critical Network Protection:** Secure internet-facing and air-gapped networks through monitoring, segregation, and access controls.

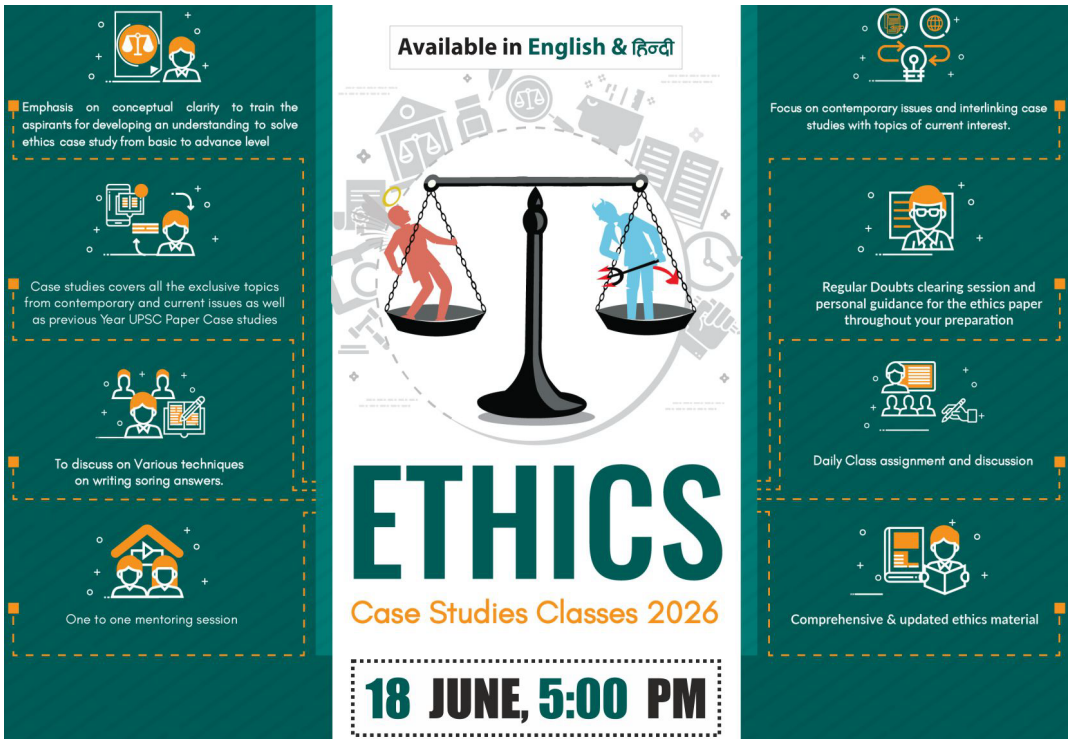
4.5. KEYWORDS

Keywords			
Defence Modernisation	Atmanirbhar Bharat	Jointness	Integration
Theatre Commands	Integrated Theatre Commands (ITCs)	Theaterisation	Chief of Defence Staff (CDS)
Department of Military Affairs (DMA)	Force Multiplication	Network-Centric Warfare	Capability Development
Multi-Domain Operations (MDO)	Joint Operations	Integrated Battle Space	Decision Dominance
Information Warfare	Electronic Warfare	Cognitive Warfare	Hybrid Warfare
Cyber Warfare	Cyberspace Operations	Cyber Defence	Cyber Deterrence
Defence Cyber Agency (DCA)	Defence Communication Network (DCN)	Situational Awareness	Real-Time Intelligence
Artificial Intelligence	Autonomous Systems	Quantum Technologies	Emerging Technologies
ISR (Intelligence, Surveillance and Reconnaissance)	Space Domain	Maritime Domain	Air-Land Integration
Mission-Oriented Forces	Interoperability	Technology-Centric Warfare	Strategic Autonomy

4.6. PRACTISE QUESTION

Cyberspace has emerged as an independent domain of warfare. Examine its significance for India's national security.

Introduction	Body Part: 1	Body Part: 2	Conclusion
Introduce cyberspace operations.	Strategic importance and applications.	Emerging challenges and vulnerabilities.	Need for strong cyber deterrence and defence.


Available in English & हिन्दी
Emphasis on conceptual clarity to train the aspirants for developing an understanding to solve ethics case study from basic to advance level
Case studies covers all the exclusive topics from contemporary and current issues as well as previous Year UPSC Paper Case studies
To discuss on Various techniques on writing soring answers.
One to one mentoring session
ETHICS
Case Studies Classes 2026
18 JUNE, 5:00 PM
Focus on contemporary issues and interlinking case studies with topics of current interest.
Regular Doubts clearing session and personal guidance for the ethics paper throughout your preparation
Daily Class assignment and discussion
Comprehensive & updated ethics material

5. MISCELLANEOUS

5.1. THE WASSENAAR ARRANGEMENT

Why in the News?

The growing proliferation of emerging technologies such as Artificial Intelligence (AI) in the military domain poses significant challenges to the existing control mechanisms of the Wassenaar Arrangement.

About the Wassenaar Arrangement

- The **Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies** is a multilateral export control regime established in **1996** which succeeded the Cold War-era **CoCom (Coordinating Committee for Multilateral Export Controls)**.
- It is the first global arrangement focused on export controls for **conventional weapons** and **dual-use goods and technologies** (items having both civilian and military applications)
- **Participating States:** Currently, there are **42 Participating States** in the Wassenaar Arrangement. **India was admitted as a member in 2017**

Dual-use Goods

- These are items that are primarily intended for civilian applications but have the potential to be used for military purposes.

Examples:

- **Electronics & Computing**: High-performance computers, lasers, radars, telecommunications, information security, navigation, avionics, and sensor systems with both civilian and military applications.
- **Space & Aerospace Technology**: Civilian space-launch equipment, materials, and software that can also support ballistic missile and UAV development.
- **Chemical & Biological Equipment**: Precursor chemicals and advanced biological research tools that could be diverted for chemical or biological weapons.
- **Software & Digital Infrastructure**: Intrusion software, cloud computing, SaaS, and AI technologies that can be misused for surveillance, profiling, cyber operations, and human rights abuses.

Challenges of the Wassenaar Arrangement

- **Outdated Export Concept:** Designed for physical transfers, making regulation of cloud-based and remote technology access difficult.
- **Cloud & SaaS Gaps:** Struggles to classify remote software access, APIs, and SaaS services as exports.
- **Consensus-Based Gridlock:** Any member can block reforms, slowing updates to control lists and rules.
- **Voluntary Implementation:** National discretion leads to uneven enforcement and regulatory loopholes.
- **Lack of Agility:** Unable to keep pace with rapid advances in AI, cloud computing, and digital technologies.
- **Limited Human Rights Focus:** Traditional emphasis on military and WMD-related controls inadequately addresses digital surveillance and repression technologies.
- **Resistance to Reforms:** Some states oppose stricter controls, citing concerns over innovation, sovereignty, and industry regulation.
- **Institutional Vulnerabilities:** Dependence on annual in-person meetings can disrupt decision-making during crises.
- **Geopolitical Pressures:** Rising global tensions and **US/EU unilateral export-control initiatives outside the WA framework** challenge its relevance, legitimacy, and cohesion.

Reforms Needed in the Wassenaar Arrangement

- **Expand Control Lists:** Include technologies enabling large-scale surveillance, biometric networks, profiling, and cross-border data systems, while permitting legitimate uses under strict safeguards.
- **Redefine "Export":** Treat remote access, authorization, administration rights, and API-based access to controlled technologies as exports.
- **Human Rights-Based End-Use Controls:** Incorporate risks of mass surveillance, repression, and human rights abuses into licensing decisions.

- **Move Towards Binding Obligations:** Participating states should adopt a binding treaty with minimum licensing standards, mandatory export denials for high-risk jurisdictions, and peer-review mechanisms.
- **Enhance Information Sharing:** Develop interoperable systems, shared watchlists, and real-time alerts among member states.
- **Develop Domain-Specific Regimes:** Establish specialized frameworks for AI, cyber weapons and digital surveillance technologies.

Other Export Control Mechanisms

- **Missile Technology Control Regime (MTCR):** Created in 1987, the MTCR seeks to prevent the proliferation of missiles and uncrewed aerial vehicles (UAVs) capable of delivering chemical, biological or nuclear weapons.
  - It currently consists of 35 participating states.
  - India is a member since 2016.
- **The Australia Group (AG):** Formed in 1985 on an initiative by Australia, this regime coordinates and harmonizes export controls to reduce the risk of chemical and biological weapons proliferation
  - It has 43 participants
  - India is a member since 2018.
- **The Nuclear Suppliers Group (NSG):** Established in 1974, the NSG implements guidelines for export controls on nuclear and nuclear-related material, equipment, software and technology.
  - It currently has 48 participating governments.
  - India is not a member.

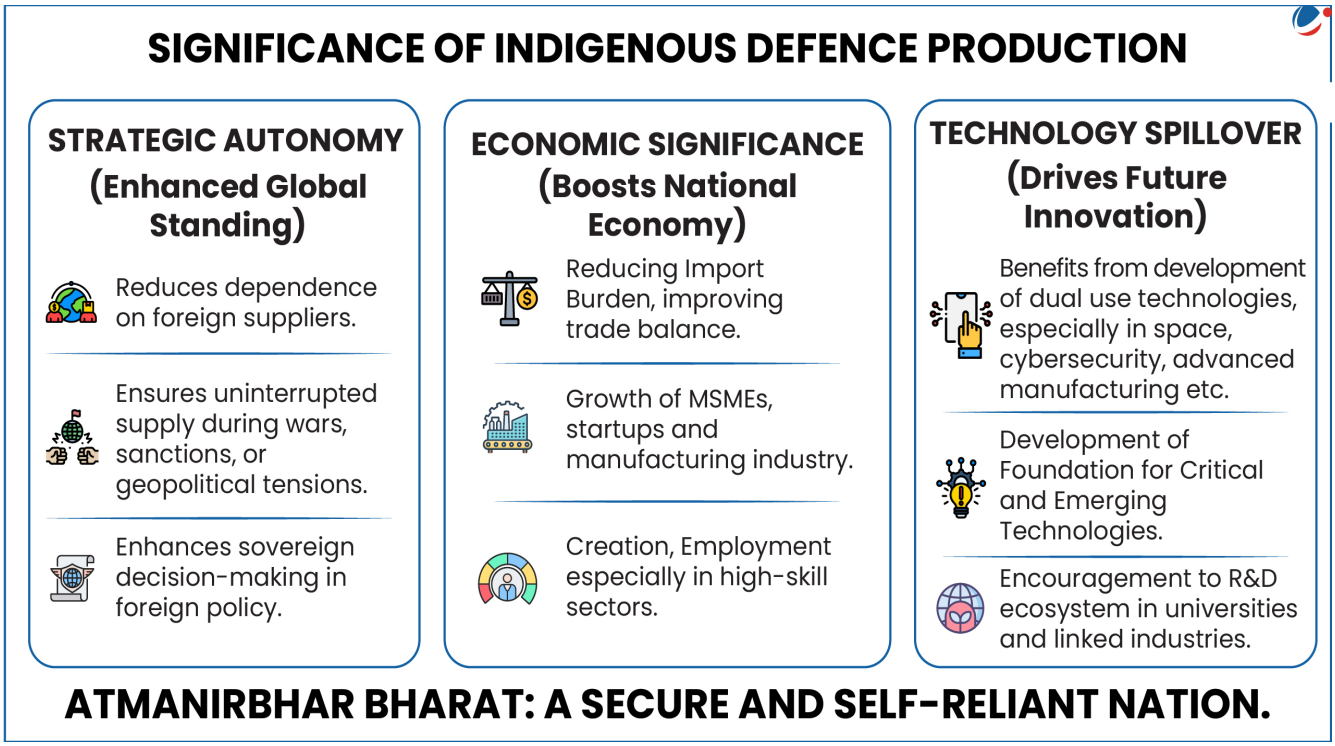
5.2. INDIA'S DEFENCE INDUSTRY

Why in the News?

Defence Minister reiterated the Government's commitment to achieve Aatmanirbharta in defence manufacturing and make the country a global defence production hub.

Defence Manufacturing Ecosystem in India

- **Production:** FY 2024-25 saw **record production at Rs 1.54 lakh crore**, up 174% from 2014-15.
  - DPSUs contributed **77%**, while the **private sector added 23%.**
  - **65% of military equipment** is now **made domestically.**
  - The private sector share in defence production is a **record** marking **third consecutive year** of **increasing private sector** involvement.
- **Exports:** Over the past decade, defence exports have grown exponentially, marking a **34-fold increase since 2013-14.**
  - The MoD aims for **Rs 50,000 crore in annual exports by 2029.**
  - **Key Markets:** India now supplies **over 100 countries**.
    - **Top three destination markets (**In 2023-24): United States, France and Armenia.
    - India has also secured **major strategic partnerships in Southeast Asia,** such as supplying the **BrahMos missile system to the Philippines,** alongside exporting to friendly South Asian nations like Sri Lanka, Nepal, and Bhutan.
- **Key Export Products: Missiles and Air Defence (**BrahMos supersonic cruise missiles, Akash SAMs); **Aviation and Drones (**Dornier-228 aircraft, Chetak helicopters); **Artillery and Munitions (**Howitzers); **Naval and Infantry Gear (**Fast interceptor boats, offshore patrol vessels, radars, thermal imagers, and bulletproof jackets).
- **Startups:** Funding for India's military-tech start-ups has risen 61 times from Rs. 27 crore in 2016 to Rs. 1,653 crore in 2025, with total investments reaching Rs. 5,248 crore.


SIGNIFICANCE OF INDIGENOUS DEFENCE PRODUCTION
STRATEGIC AUTONOMY (Enhanced Global Standing)
Reduces dependence on foreign suppliers.
Ensures uninterrupted supply during wars, sanctions, or geopolitical tensions.
Enhances sovereign decision-making in foreign policy.
ECONOMIC SIGNIFICANCE (Boosts National Economy)
Reducing Import Burden, improving trade balance.
Growth of MSMEs, startups and manufacturing industry.
Creation, Employment especially in high-skill sectors.
TECHNOLOGY SPILLOVER (Drives Future Innovation)
Benefits from development of dual use technologies, especially in space, cybersecurity, advanced manufacturing etc.
Development of Foundation for Critical and Emerging Technologies.
Encouragement to R&D ecosystem in universities and linked industries.
ATMANIRBHAR BHARAT: A SECURE AND SELF-RELIANT NATION.

Government Initiatives for Defence Manufacturing

- **Budgetary Prioritization:** For FY2025-26, the **Ministry of Defence has earmarked 75% of its modernization budget (₹1.11 lakh crore)** specifically for procurement from Indian firms.
- **Defence Industrial Corridors (DICs):** Two dedicated DICs have been established in Uttar Pradesh and Tamil Nadu.
- **Positive Indigenisation Lists:** The government has issued **Positive Indigenisation Lists** that limit imports and encourage local manufacturing.
- **Innovations for Defence Excellence (iDEX):** By engaging MSMEs, startups, individual innovators, R&D institutes, and academia, iDEX has provided grants of up to ₹1.5 crore to support the development of cutting-edge technologies.
- **Liberalized FDI Policy:** Allows up to 74% FDI under the automatic route and beyond 74% (up to 100%) through the Government route.
- **Technology Development Fund (TDF):** Established to promote self-reliance in Defence Technology as a part of the 'Make in India' initiative.
- **DefExpo:** It was conceptualised in 1998 and has evolved as a flagship platform for showcasing India's defence industrial capabilities and promoting defence exports.

Challenges to Atmanirbharata in Defence Manufacturing

- **Limited Fiscal Space:** Out of the total allocation made to the Ministry of Defence, only 27.95% of the Defence Budget allocation is for capital expenditure.
- **Import Dependence:** India continues to depend on foreign suppliers for critical technologies and high-end platforms such as aero engines, propulsion modules, advanced materials, sensors etc.
- **Technological:** Foreign **Original Equipment Manufacturers (OEMs) are protective of intellectual property** and **provide limited technology transfer**.
  - Limited technological depth in **emerging defence technologies** including AI, hypersonics, cyber warfare, and stealth tech, etc.
- **Fragmentation of Defence Innovation Landscape:** Although India has created multiple DRDO–academia–industry collaboration frameworks, defence R&D remains fragmented in practice, with cooperation often project-specific rather than system-wide.

- Unlike in Western countries, where most R&D occurs in the private sector, in India, it is dominated by the government and public-sector entities.

- **Lack of Input Enablers:** Advanced defence production requires reliable capital investments, precision machining and tooling, testing facilities, materials laboratories and secure digital networks.
- **Insufficient Skilling:** While India produces a large number of engineering and science graduates each year, persistent concerns remain regarding their employability.

Conclusion

Atmanirbharta in Defence has expanded production numbers, diversified the supplier base, and altered the political discourse and public awareness around defence production. By deepening public–private synergy, prioritising critical technologies and positioning exports as a strategic instrument of diplomacy, India can transition from being a major arms importer to a trusted global defence manufacturing hub. In doing so, defence indigenisation will not only enhance national security but also become a catalyst for industrial modernisation, strategic autonomy and long-term economic resilience.

5.3. KEYWORDS

Keywords			
Wassenaar Arrangement	Dual-Use Goods	Export Controls	Conventional Arms
Missile Technology Control Regime (MTCR)	Australia Group	Nuclear Suppliers Group (NSG)	Emerging Technologies
Artificial Intelligence (AI)	Cloud Computing	Cyber Weapons	Digital Surveillance
Global Nuclear Order	Nuclear Deterrence	Nuclear Taboo	Strategic Stability
Nuclear Non-Proliferation Treaty (NPT)	Treaty on the Prohibition of Nuclear Weapons (TPNW)	Arms Control	Nuclear Disarmament
Credible Minimum Deterrence	Nuclear Modernisation	AI-Enabled Warfare	Nuclear Risk Reduction
Atmanirbhar Bharat	Defence Manufacturing	Defence Exports	Strategic Autonomy
Defence Industrial Corridors	Positive Indigenisation Lists	iDEX	Technology Development Fund (TDF)
Defence Public Sector Undertakings (DPSUs)	Public-Private Partnership	Technology Transfer	Defence Innovation
Defence Startups	Defence R&D	Critical Technologies	Defence Indigenisation

5.4. PRACTICE QUESTION

Defence indigenisation is critical for achieving strategic autonomy and strengthening national security. Examine.

Introduction	Body Part: 1	Body Part: 2	Conclusion
Introduce defence indigenisation.	Achievements and government initiatives.	Challenges and areas requiring attention.	Need for innovation-led self-reliance.

6. APPENDIX: QUICK FACTS

1. Left-Wing Extremism (LWE)

Particulars	Quick Facts
Meaning	Maoist/Naxalite movement seeking to overthrow the democratic state through armed struggle.
Origin	Naxalbari uprising (1967), West Bengal.
Affected Area	Red Corridor across central and eastern India.
Latest Trend	LWE violence reduced by about 89% (2010–2025); affected districts reduced to two.
Drivers	Jal-Jangal-Jameen issues, tribal alienation, socio-economic deprivation, governance deficits.
Government Measures	National Policy & Action Plan (2015), SAMADHAN Strategy, Police Modernisation, Civic Action Programme, Special Central Assistance.
Challenges	Difficult terrain, technology misuse, trust deficit, arms availability.
Way Forward	Implement FRA & PESA effectively, intelligence-led policing, tribal development, Centre–State coordination.

2. Armed Forces (Special Powers) Act (AFSPA), 1958

Particulars	Quick Facts
Purpose	Empowers armed forces in disturbed areas.
Current Coverage	Parts of Nagaland, Manipur, Assam, Arunachal Pradesh and J&K (as applicable).
Important Judgments	Naga People's Movement (1997); EEVFAM (2016); Sebastian Hongray (1984).
Committees	Jeevan Reddy Committee, Second ARC, Justice Verma Committee.
Issues	Human rights concerns, accountability, prolonged deployment.
Way Forward	Periodic review, stronger oversight, improved policing and community participation.

3. Insurgency in North-East India

Particulars	Quick Facts
Major Causes	Ethnic rivalries, porous borders, AFSPA-related alienation, governance deficits.
Examples	Meitei–Kuki conflict, NSCN factions, Assam–Mizoram dispute.
Peace Measures	Bodo Accord, Karbi Anglong Agreement, NLFT Agreement.
Connectivity	UDAN, Vande Bharat, Bogibeel Bridge, Sela Tunnel, Kaladan Project.
Way Forward	Political dialogue, development, cultural integration, human-rights based security.

4. High-Powered Demography Mission

Particulars	Quick Facts
Objective	Address illegal immigration and infiltration.
Security Concerns	Terror links, trafficking, demographic imbalance, smuggling.
Existing Measures	Immigration & Foreigners Act 2025, NRC, CAA, CIBMS, border fencing, Foreigners Tribunals.
Way Forward	Smart surveillance, biometric databases, National Refugee Law, bilateral repatriation agreements.

5. Online Radicalisation

Particulars	Quick Facts
Meaning	Adoption of extremist views through digital platforms leading to violence or terrorism.
Push Factors	Unemployment, marginalisation, discrimination, loss of faith in institutions.
Pull Factors	Online propaganda, monetary incentives, exploitation of conflicts.
Facilitators	Echo chambers, micro-targeting, encrypted platforms, cybercrime, terror financing.
Challenges	Dark Web anonymity, encrypted messaging, lack of universal definition of terrorism, rapid internet penetration.
Indian Measures	IT Act 2000, I4C, MeitY URL blocking, Operation SADBHAVANA, Operation Pigeon, Sahi Raasta.
Global Measures	Tech Against Terrorism, Christchurch Call, INTERPOL, Bharatpol.
Way Forward	Counter-narratives, stronger platform regulation, rehabilitation, global intelligence cooperation.

6. Cryptocurrencies & Smuggling

Particulars	Quick Facts
Key Concern	Stablecoins and cryptocurrencies increasingly used for drug and gold smuggling.
Reasons	Decentralisation, pseudonymity, Dark Web markets, VPN-enabled wallets, off-book payments.
Indian Framework	Finance Act 2022 (30% VDA tax); PMLA coverage extended to VDAs (2023).
Global Framework	FATF AML/CFT standards.
Way Forward	Mandatory KYC, blockchain forensics, AI-enabled transaction analytics, international cooperation.

7. AI in Internal Security

Particulars	Quick Facts
Applications	Predictive policing, surveillance, behavioural analytics, crime pattern recognition.
Major Risks	Privacy, algorithmic bias, black-box decisions, automation bias, scalability of errors.
Legal Context	Right to Privacy (Puttaswamy), DPDP Act 2023.
Way Forward	Human-in-the-loop, AI audits, ethical governance, NCR&IC capacity building, INTERPOL cooperation.

8. Data Protection

Particulars	Quick Facts
Need	Protect privacy, strengthen digital governance, secure critical infrastructure.
Importance	Supports UIDAI, NATGRID, Aadhaar, UPI and digital economy.
Challenges	Techno-colonialism, cyber threats, localisation issues, digital literacy gaps.
Major Initiatives	DPDP Act 2023, IT Rules 2021, Cyber Surakshit Bharat, PMGDISHA.
Way Forward	Digital sovereignty, anonymisation, CERT-In training, learn from GDPR.

9. Critical Information Infrastructure (CII)

Particulars	Quick Facts
Definition	IT resources whose disruption impacts national security, economy or public safety.
Critical Sectors	Power, banking, telecom, transport and government.

Threats	State-sponsored attacks, IoT vulnerabilities, AI-enabled attacks, mobile malware.
Institutions	NCIIPC, CERT-In, NCCC, I4C.
Exercises	Cyber Suraksha by Defence Cyber Agency.
Way Forward	Cyber Kill Chain approach, PPP, indigenous cyber tools, resilience strategy.

10. Cybercrime in India

Particulars	Quick Facts
Current Status	Internet users crossed 100 crore; cyber fraud, ransomware and AI-enabled scams rising.
Cybersecurity Industry	~US$20 billion industry with 400+ startups and ~6.5 lakh professionals.
Major Threats	Phishing, ransomware, financial fraud, identity theft, malware, supply-chain attacks.
Institutions	CERT-In, NCIIPC, I4C, NCCC, Cyber Swachhta Kendra.
Legal Framework	Information Technology Act, Digital Personal Data Protection Act, Bharatiya Nyaya Sanhita provisions.
Way Forward	Cyber awareness, skilled manpower, stronger incident reporting and indigenous technologies.

11. Contemporary & Emerging Cyber Threats

Particulars	Quick Facts
Emerging Risks	AI-enabled attacks, ransomware-as-a-service, cloud attacks, IoT vulnerabilities.
Critical Targets	**Power grids, banking, telecom, defence, healthcare and government databases.**
Need	**Whole-of-government cyber resilience and real-time threat intelligence.**

12. Quantum-related Threats

Particulars	Quick Facts
Harvest Now Decrypt Later	Encrypted data stolen today for future decryption by quantum computers.
Signature Forgery	Quantum computing may compromise digital signatures and certificates.
Zero-day Risks	New cryptographic vulnerabilities may emerge.
Response	Migration to Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD).

13. AI-related Cyber Threats

Particulars	Quick Facts
Threats	Deepfakes, automated phishing, AI malware, synthetic identity fraud.
Concerns	Automation of cyberattacks, misinformation, adversarial AI.
Countermeasures	AI-assisted threat detection, algorithm audits, secure AI governance.

14. Digital Sovereignty

Particulars	Quick Facts
Meaning	Nation's ability to control its digital infrastructure, data and technologies.
Importance	Reduces dependence on foreign platforms and strengthens strategic autonomy.
Indian Initiatives	India Stack, ONDC, Semiconductor Mission, National Quantum Mission.
Way Forward	Indigenous hardware, trusted telecom, domestic cloud infrastructure.

15. UN Convention Against Cybercrime

Particulars	Quick Facts
Purpose	International cooperation against cyber-enabled crimes.
Objectives	Evidence sharing, capacity building, cross-border investigations.
Concerns	Balancing security, privacy and human rights.

16. Quantum Cyber Readiness

Particulars	Quick Facts
Need	Prepare institutions for quantum-era cyber threats.
Key Measures	Crypto inventory, migration roadmap, hybrid encryption, workforce training.
Indian Focus	National Quantum Mission, C-DOT initiatives, quantum-safe communication.

17. Terrorism

Particulars	Quick Facts
Definition	Use or threat of violence to create fear and achieve political, ideological or religious objectives.
Emerging Trends	Hybrid terrorism, drone-enabled attacks, AI-assisted propaganda, lone-wolf attacks.
Challenges	No universally accepted definition, terror financing, encrypted communication, cross-border support.
Indian Framework	UAPA 1967, NIA Act, NATGRID, Multi Agency Centre (MAC), NSG.
Way Forward	Intelligence integration, counter-radicalisation, international cooperation, technology-enabled surveillance.

18. State-Sponsored Terrorism

Particulars	Quick Facts
Meaning	Support by a state to terrorist groups through funding, training or safe havens.
Concerns	Cross-border infiltration, proxy warfare, regional instability.
Response	Diplomatic isolation, FATF pressure, stronger border management.

19. White Collar Terrorism

Particulars	Quick Facts
Meaning	Large-scale economic crimes threatening national security and financial stability.
Examples	Financial fraud, cyber-enabled fraud, corruption, shell companies.
Response	Stronger regulatory oversight, forensic audits, inter-agency coordination.

20. Transnational Organised Crimes (TNOCs)

Particulars	Quick Facts
Types	Drug trafficking, human trafficking, cybercrime, migrant smuggling, money laundering.
Challenges	Jurisdictional issues, porous borders, organised criminal networks.
International Mechanisms	UNTOC, INTERPOL, FATF.
Way Forward	Cross-border intelligence sharing and stronger AML/CFT framework.

21. Money Laundering

Particulars	Quick Facts
Stages	Placement, Layering and Integration.
Impact	Terror financing, organised crime, market distortion and corruption.
Indian Law	Prevention of Money Laundering Act (PMLA), 2002; Enforcement Directorate.
Global Standards	FATF Recommendations.
Way Forward	Beneficial ownership transparency, digital financial intelligence, stronger enforcement.

22. Drug Trafficking

Particulars	Quick Facts
Major Routes	Golden Triangle and Golden Crescent affecting India.
Threats	Narco-terrorism, youth addiction, organised crime, public health burden.
Indian Law	NDPS Act, 1985.
Institutions	NCB, DRI, Coast Guard, BSF, state police.
Way Forward	Border surveillance, financial tracking, regional cooperation and rehabilitation.

23. Geospatial Data & National Security

Particulars	Quick Facts
Importance	Supports surveillance, disaster management, military planning, navigation and infrastructure development.
Indian Capabilities	NavIC, Bhuvan, PM Gati Shakti, SVAMITVA, National Geospatial Policy 2022, EOS satellites.
Threats	Data misuse, cyber espionage, mapping sensitive installations.
Way Forward	Secure indigenous geospatial infrastructure, AI-enabled analytics and stronger data governance.

24. Hybrid Warfare

Particulars	Quick Facts
Meaning	Combination of conventional, irregular, cyber, economic and information warfare.
Tools	Cyberattacks, disinformation, proxy groups, economic coercion, drones.
Examples	Information warfare, infrastructure sabotage, cyber campaigns.
Response	Whole-of-government resilience, cyber preparedness and strategic communication.

25. Grey-Zone Warfare

Particulars	Quick Facts
Meaning	Coercive actions below the threshold of conventional war.
Methods	Lawfare, cyber intrusions, maritime coercion, economic pressure, influence operations.
Challenge	Ambiguity makes attribution and retaliation difficult.
Way Forward	Integrated intelligence, diplomatic coordination and rapid response mechanisms.

26. Biosecurity & Biological Weapons Convention

Particulars	Quick Facts
Biosecurity	Protection against accidental or deliberate misuse of biological agents.

Convention	Biological Weapons Convention (BWC) prohibits development and stockpiling of biological weapons.
Challenges	Synthetic biology, dual-use research, weak verification.
Way Forward	Strengthen biosurveillance, laboratory security and international cooperation.

27. Space Weaponisation

Particulars	Quick Facts
Threats	ASAT weapons, satellite jamming, spoofing and cyberattacks on space assets.
Indian Steps	Mission Shakti, Defence Space Agency, ISRO capabilities.
Way Forward	Space situational awareness, resilient satellite networks and global norms.

28. Border Security

Particulars	Quick Facts
Major Challenges	Cross-border terrorism, infiltration, illegal migration, narcotics, drone incursions.
Initiatives	CIBMS, border fencing, smart surveillance, BIM Scheme.
Institutions	BSF, ITBP, Assam Rifles, SSB.
Way Forward	Technology-enabled border management and intelligence integration.

29. Sudarshan Chakra Mission

Particulars	Quick Facts
Purpose	Air Defence system aimed at neutralising enemy defence infiltrations and enhancing India's offensive capabilities.
Focus	Indegeneous technology and Air superiority

30. Quantum Technologies in Armed Forces

Particulars	Quick Facts
Applications	Quantum communication, sensing, navigation and secure military networks.
Indian Initiatives	National Quantum Mission, quantum communication research.
Benefit	Resilient command-and-control and quantum-secure communications.

31. Advanced Technology in Border Management

Particulars	Quick Facts
Technologies	UAVs, AI analytics, smart fencing, thermal imagers, radars, sensors.
Objective	Improve surveillance, reduce infiltration and strengthen situational awareness.

32. Maritime Security

Particulars	Quick Facts
Importance	Protects sea lines of communication (SLOCs), trade, energy security and EEZ interests.
Major Threats	Piracy, maritime terrorism, trafficking, illegal fishing, Chinese naval presence.
Indian Initiatives	SAGAR, IFC-IOR, Coastal Surveillance Network, Information Fusion Centre, Sagar Kavach.
Institutions	Indian Navy, Indian Coast Guard, Marine Police.
Way Forward	Maritime Domain Awareness, Blue Economy security and Indo-Pacific partnerships.

33. Defence Modernisation

Particulars	Quick Facts
Need	Prepare armed forces for multi-domain, technology-driven warfare.
Major Initiatives	Atmanirbhar Bharat, DAP 2020, iDEX, Mission DefSpace, ADITI, Defence Corridors.
Challenges	Budget constraints, legacy platforms, import dependence, procurement delays.
Way Forward	Indigenisation, AI, robotics, quantum, hypersonics and private sector participation.

34. Theaterisation of Defence

Particulars	Quick Facts
Meaning	Integration of Army, Navy and Air Force under unified theatre commands.
Objectives	Joint planning, resource optimisation and faster operational response.
Benefits	Improved interoperability and efficient command structure.
Challenges	Inter-service integration and organisational reforms.

35. Joint Doctrine for Multi-Domain Operations

Particulars	Quick Facts
Concept	Integrated employment of military capabilities across land, air, sea, cyber and space.
Focus	Network-centric warfare, AI-enabled decision-making, joint operations.
Significance	Enhances deterrence and operational effectiveness.

36. Joint Doctrine for Cyberspace Operations

Particulars	Quick Facts
Objective	Secure military cyber infrastructure and conduct cyber operations.
Key Elements	Cyber defence, resilience, offensive cyber capability, information assurance.
Need	Growing cyber threats against defence networks.

37. Wassenaar Arrangement

Particulars	Quick Facts
Nature	Multilateral export control regime for conventional arms and dual-use goods & technologies.
Objective	Promote transparency and responsible exports.
India	Member since 2017; strengthens high-technology trade and export controls.

38. India's Defence Industry

Particulars	Quick Facts
Vision	Self-reliant defence manufacturing under Atmanirbhar Bharat.
Major Initiatives	Defence Industrial Corridors, iDEX, Positive Indigenisation Lists, FDI reforms.
Exports	Record growth in defence exports with increasing global footprint.
Way Forward	Boost R&D, MSMEs, startups, private participation and advanced manufacturing.

Copyright © by Vision IAS
All rights are reserved. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior permission of Vision IAS.

VISIONIAS
INSPIRING INNOVATION

ANNOUNCING

MAINS EDGE 45

for Mains 2026

Marks Improvement Classes & Mentoring Programme

Smart Answer Writing Intervention

Better Preparation. Better Answers. Better Marks.

45 Days | GS I–IV + Essay | Offline & Online

Highlights

- **90** Workbooks
- 2 Answers Evaluated Daily within 24 Hours
- Weekly Faculty Mentoring for GS and Optional
- Vision Answer Writing Lab | 8 AM – 8 PM
- 4 GS Paper-wise Tests + Essay Guidance
- Progress Tracking + Faculty Notes

*Paper-wise Modules also available

10 June, 11 AM

www.visionias.in/upsc-mains-edge

Scan Qr or Visit

Smriti Ma'am

Subject
Society, Social Justice, Ethics, Essay

Rajesh Sir

Subject
Geography & DM

Jatin Sir

Subject
Polity & Governance, Security, Ethics

Piyush Sir

Subject
Economics, Ethics Case Study

Abhishek Sir

Subject
Environment, S&T

Shivi Ma'am

Subject
History

Kanishk Sir

Subject
International Relations

VISIONIAS
INSPIRING INNOVATION

MASTER THE ART of ESSAY WRITING for UPSC CSE MAINS

The Essay paper in UPSC Mains is where ranks are made or lost. Wide score variations among aspirants make it one of the most decisive yet underestimated papers in the entire UPSC journey. The difference between an average essay and a scoring one lies not in what you know but in how you think, structure, and present.

THE ART OF WRITING AN IMPACTFUL ESSAY

Choose Wisely — Select a topic you can explore with depth and balance across multiple dimensions. Avoid topics that seem exciting but lack content depth.

Begin Powerfully — The introduction is your first impression. Anchor it with a compelling quote, anecdote, or thought-provoking contrast that immediately draws the examiner in.

Cracking the Philosophical Essay — Abstract and idea-based topics, increasingly dominant in recent UPSC papers, demand more than facts. They require a clear point of view, conceptual clarity, and the ability to interpret the topic from a broader philosophical, ethical, or human perspective & not merely through social, economic, or political lenses alone.

Build with Depth — The body must weave social, political, economic, ethical, historical, and contemporary perspectives into a coherent, flowing argument. Each paragraph should connect logically to the next, substantiated with facts, data, or relevant examples.

Conclude with Vision — Summarise your central argument, offer a forward-looking insight, and leave a lasting impression. An optimistic, prescriptive close tied back to your introduction creates a complete, coherent essay.

Practice with Feedback — Essay writing sharpens only through regular writing and honest, constructive feedback from mentors and peers.

INTRODUCING

THE ESSAY ENRICHMENT PROGRAM 2026

To help aspirants build this craft systematically, VisionIAS presents the Essay Enrichment Program 2026- a focused, structured program.

Starting 9 June at 5 PM

Guided by experienced VisionIAS faculty

Smriti Shah Ma'am

KEY HIGHLIGHTS:

- 5 live-offline interactive classes
- Covers philosophical and information-based essay types
- 5 mini tests with detailed, personalised feedback
- Faculty led mentoring group sessions
- Supplementary reference material in soft copy
- PYQ analysis to align with UPSC expectations

Your essay. Your rank. Start building it right.

Register for the Program
https://visionias.in/essay/

Download Essay Topper Copies
https://visionias.in/resources/toppers-answer-copy/

Heartiest *Congratulations* to all successful candidates

7 in Top 10 & 71 in Top 100 Selections in **CSE 2025** *from various programs of* VisionIAS

STRONG FOUNDATION, STRONGER RESULT | **A Legacy of Performance Excellence**

10 in Top 100 FROM OUR CLASSROOM FOUNDATION COURSE

5 AIR — ISHAN BHATNAGAR

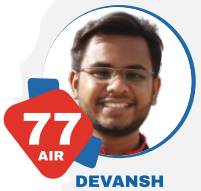
31 AIR — ARYAN YADAV

46 AIR — SHAMBHAVI TIWARI

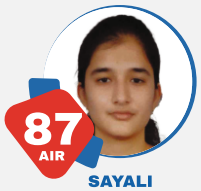
48 AIR — ANIKET RAJAN

60 AIR — ANANYA YADAV

61 AIR — ALASE HRISHIKESH


77 AIR — DEVANSH GUPTA

85 AIR — ISHA BARAK


87 AIR — SAYALI BHIKA PAGAR

92 AIR — GARIMA SINGH

Scan to Know More & REGISTER for FREE COUNSELING connect with our Expert 8468022022

Previous Years' GS FOUNDATION CLASSROOM COURSE Selections

UPSC CSE 2024

2 AIR — HARSHITA GOYAL

3 AIR — DONGRE ARCHIT PARAG

UPSC CSE 2022

7 AIR — WASEEM AHMAD BHAT

UPSC CSE 2021

5 AIR — UTKARSH DWIVEDI

UPSC CSE 2020

1 AIR — SHUBHAM KUMAR

8 AIR — JIVANI KARTIK NAGJIBHAI

LIVE/ONLINE Classes Available

www.visionias.in

Scan QR code for instant personalized mentoring

Foundation Course
GENERAL STUDIES
PRELIMS cum MAINS

2027, 2028 & 2029

DELHI: 30 JUNE, 8 AM | 9 JULY, 11 AM | 16 JULY, 8 AM
22 JULY, 5 PM | 23 JULY, 11 AM | 24 JULY, 2 PM | 30 JULY, 8 PM

GTB NAGAR : 17 JULY, 6 PM | 19 JULY, 8 AM

AHMEDABAD: 15 JUNE | BENGALURU: 20 JULY | BHOPAL: 2 JUNE | HYDERABAD: 13 JULY
JAIPUR: 17 JUNE, 22 JUNE | JODHPUR: 15 MAY | LUCKNOW: 15 JULY | PUNE: 15 JULY

फाउंडेशन कोर्स सामान्य अध्ययन 2026

▸ प्रारंभिक, मुख्य परीक्षा और निबंध के लिए महत्वपूर्ण सभी टॉपिक का विस्तृत कवरेज

DELHI : 15 जुलाई, 8 AM | **JAIPUR : 18 मई & 22 जून** | **JODHPUR : 15 मई**

DELHI: GMMR 33, Pusa Road, Near Karol Bagh Metro Station, Opposite Pillar No. 113, Delhi – 110005 | **CONTACT:** 8468022022, 9019066066

AHMEDABAD | BENGALURU | BHOPAL | CHANDIGARH | GUWAHATI | HYDERABAD | JAIPUR | JODHPUR | LUCKNOW | PRAYAGRAJ | PUNE | RANCHI

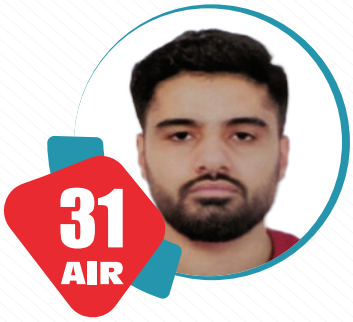
10 in top 100

Selections from our

GS Foundation Classroom Course

in CSE 2025

ISHAN BHATNAGAR



ARYAN YADAV

SHAMBHAVI TIWARI

ANIKET RANJAN

ANANYA RANA

ALASE HRISHIKESH

DEVANSH GUPTA

ISHA BARAK

SAYALI BHIKA PAGAR

GARIMA SINGH

Previous Years' GS Foundation Classroom Course Selections

UPSC CSE 2024

HARSHITA GOYAL

DONGRE ARCHIT PARAG

UPSC CSE 2022

WASEEM AHMAD BHAT

UPSC CSE 2021

UTKARSH DWIVEDI

UPSC CSE 2020

SHUBHAM KUMAR

JIVANI KARTIK NAGJIBHAI

enquiry@visionias.in | /c/VisionIASdelhi | /visionias.upsc | /vision _ias | VisionIAS_UPSC

DELHI

GMMR ENQUIRY & CLASSROOM CENTER
33, Pusa Road,
Near Karol Bagh Metro Station,
Opposite Pillar No. 113,
Delhi - 110005

MUKHERJEE NAGAR CENTER
Plot No. 857, Ground Floor,
Mukherjee Nagar, Opposite Punjab & Sindh Bank, Mukherjee Nagar

GTB NAGAR CENTER
Classroom & Enquiry Office,
above Gate No. 2, GTB Nagar Metro Building, Delhi - 110009

FOR DETAILED ENQUIRY
Please Call:
+91 8468022022,
+91 9019066066

AHMEDABAD | BENGALURU | BHOPAL | CHANDIGARH | DELHI | GUWAHATI | HYDERABAD | JAIPUR | JODHPUR | LUCKNOW | PRAYAGRAJ | PUNE | RANCHI